(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-88534
(P2004-88534A)
(43)公開日　平成16年3月18日(2004.3.18)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/32	H04L	9/00	675B	5B058
B65G 61/00	B65G	61/00	210	5J104
G06F 17/60	B65G	61/00	522	
G06K 17/00	G06F	17/60	114	
	G06F	17/60	302A	

審査請求 未請求　請求項の数 29　ＯＬ　（全 34 頁）　最終頁に続く

(21)出願番号　特願2002-248108(P2002-248108)
(22)出願日　平成14年8月28日(2002.8.28)

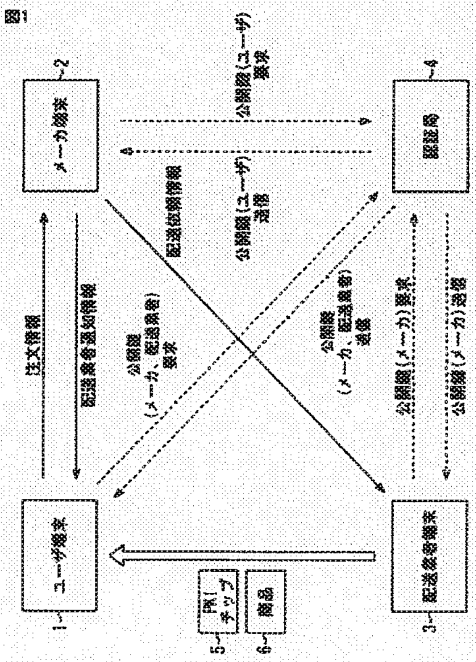
(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番３５号
(74)代理人　100082131
弁理士　稲本　義雄
(72)発明者　飯塚　健
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

Ｆターム(参考)　5B058 CA15 CA23 CA25 KA02 KA04
KA31 KA35 YA20
5J104 AA09 AA10 KA05 LA03 MA01

(54)【発明の名称】検証システムおよび方法、情報処理装置および方法、受注管理装置および方法、配送管理装置および方法、情報管理チップおよび方法、記録媒体、並びにプログラム

(57)【要約】
【課題】容易に、かつ確実に、配送されてきた商品の正当性を検証することができるようにする。
【解決手段】ユーザ端末１においては、注文が受け付けられたことを通知する情報とともに、配送業者を通知する配送業者情報がメーカ端末２から送信されてきたとき、認証局４に対して配送業者の公開鍵の発行が要求され、要求に応じて発行されてきた公開鍵が保存される。配送業者により商品とともに配送されてくるＰＫＩチップ５には、ユーザ端末１により認証局４から取得された公開鍵に対応する秘密鍵が管理されており、配送されてきた商品の確認処理として、ユーザ端末１とＰＫＩチップ５との間で、ＰＫＩチップ５の秘密鍵により生成された署名情報の検証処理が行われる。本発明は、各種の荷物を配送する配送システムに適用することができる。
【選択図】　図１

図1



【特許請求の範囲】
【請求項１】
配送されてきた商品に関連する情報を検証する情報処理装置と、前記商品とともに配送される情報管理チップからなる検証システムにおいて、
前記情報処理装置は、
前記情報管理チップにより保存されている秘密鍵に対応する公開鍵を取得する取得手段と、
無作為情報を生成する無作為情報生成手段と、
前記無作為情報生成手段により生成された前記無作為情報を、近距離無線通信を介して前記情報管理チップに送信する無作為情報送信手段と、
前記無作為情報送信手段により送信された前記無作為情報に対応するものとして前記情報管理チップにより生成された署名情報を、前記近距離無線通信を介して受信する署名情報受信手段と、
前記署名情報受信手段により受信された前記署名情報を、前記取得手段により取得された前記公開鍵を用いて検証する検証手段と
を備え、
前記情報管理チップは、
前記秘密鍵を記憶する記憶手段と、
前記商品の受取人により操作される前記情報処理装置から、前記近距離無線通信を介して送信された前記無作為情報を受信する無作為情報受信手段と、
前記記憶手段により記憶されている前記秘密鍵を用いて、前記無作為情報受信手段により受信された前記無作為情報に対応する前記署名情報を生成する署名情報生成手段と、
前記署名情報生成手段により生成された前記署名情報を、前記近距離無線通信を介して前記情報処理装置に送信する署名情報送信手段と
を備えることを特徴とする検証システム。
【請求項２】
配送されてきた商品に関連する情報を検証する情報処理装置と、前記商品とともに配送される情報管理チップからなる検証システムの検証方法において、
前記情報処理装置の情報処理方法は、
前記情報管理チップにより保存されている秘密鍵に対応する公開鍵を取得する取得ステップと、
無作為情報を生成する無作為情報生成ステップと、
前記無作為情報生成ステップの処理により生成された前記無作為情報を、近距離無線通信を介して前記情報管理チップに送信する無作為情報送信ステップと、
前記無作為情報送信ステップの処理により送信された前記無作為情報に対応するものとして前記情報管理チップにより生成された署名情報を、前記近距離無線通信を介して受信する署名情報受信ステップと、
前記署名情報受信ステップの処理により受信された前記署名情報を、前記取得ステップの処理により取得された前記公開鍵を用いて検証する検証ステップと
を含み、
前記情報管理チップの情報管理方法は、
前記秘密鍵を記憶する記憶ステップと、
前記商品の受取人により操作される前記情報処理装置から、前記近距離無線通信を介して送信された前記無作為情報を受信する無作為情報受信ステップと、
内部に記憶されている前記秘密鍵を用いて、前記無作為情報受信ステップの処理により受信された前記無作為情報に対応する前記署名情報を生成する署名情報生成ステップと、
前記署名情報生成ステップの処理により生成された前記署名情報を、前記近距離無線通信を介して前記情報処理装置に送信する署名情報送信ステップと
を含むことを特徴とする検証方法。
【請求項３】

配送されてきた商品に関連する情報を検証する情報処理装置において、
前記商品とともに配送されてきた情報管理チップにより管理されている第１の秘密鍵に対応する公開鍵を取得する取得手段と、
無作為情報を生成する無作為情報生成手段と、
前記無作為情報生成手段により生成された前記無作為情報を、近距離無線通信を介して前記情報管理チップに送信する送信手段と、
前記送信手段により送信された前記無作為情報に対応するものとして前記情報管理チップにより生成された第１の署名情報を、前記近距離無線通信を介して受信する署名情報受信手段と、
前記署名情報受信手段により受信された前記第１の署名情報を、前記取得手段により取得された前記公開鍵を用いて検証する第１の検証手段と
を備えることを特徴とする情報処理装置。
【請求項４】
前記第１の秘密鍵を用いて前記情報管理チップにより生成された、前記商品の配送に関する配送関連情報に対応する第２の署名情報を、前記配送関連情報とともに前記近距離無線通信を介して受信する配送関連情報受信手段と、
前記配送関連情報受信手段により受信された前記第２の署名情報を、前記公開鍵を用いて検証する第２の検証手段と
をさらに備え、
前記送信手段は、前記第２の検証手段により前記第２の署名情報の正当性が確認されたとき、前記無作為情報を前記情報管理チップに送信する
ことを特徴とする請求項３に記載の情報処理装置。
【請求項５】
前記第１の検証手段により前記第１の署名情報の正当性が確認されたとき、前記配送関連情報を出力する配送関連情報出力手段をさらに備える
ことを特徴とする請求項４に記載の情報処理装置。
【請求項６】
前記第１の検証手段による検証結果を出力する検証結果出力手段をさらに備える
ことを特徴とする請求項３に記載の情報処理装置。
【請求項７】
第２の秘密鍵を記憶する記憶手段と、
前記記憶手段により記憶されている前記第２の秘密鍵を用いて、前記商品の識別情報を含む商品情報、および、前記商品の注文主に関するユーザ情報に対応する第２の署名情報を生成する署名情報生成手段と、
前記商品情報、前記ユーザ情報、前記署名情報生成手段により生成された前記第２の署名情報を含む注文情報を、前記商品の受注を管理する受注管理装置に対して送信し、前記商品を注文する注文手段と
をさらに備えることを特徴とする請求項３に記載の情報処理装置。
【請求項８】
前記商品の注文が受け付けられたことが前記受注管理装置から通知されてきたとき、前記第１の秘密鍵に対応する前記公開鍵の送信を認証局に対して要求する要求手段をさらに備え、
前記取得手段は、前記要求手段による要求に応じて前記認証局から送信されてきた前記公開鍵を取得する
ことを特徴とする請求項７に記載の情報処理装置。
【請求項９】
配送されてきた商品に関連する情報を検証する情報処理装置の情報処理方法において、
前記商品とともに配送されてきた情報管理チップにより管理されている秘密鍵に対応する公開鍵を取得する取得ステップと、
無作為情報を生成する生成ステップと、

前記生成ステップの処理により生成された前記無作為情報を、近距離無線通信を介して前記情報管理チップに送信する送信ステップと、
前記送信ステップの処理により送信された前記無作為情報に対応するものとして前記情報管理チップにより生成された署名情報を、前記近距離無線通信を介して受信する受信ステップと、
前記受信ステップの処理により受信された前記署名情報を、前記取得ステップの処理により取得された前記公開鍵を用いて検証する検証ステップと
を含むことを特徴とする情報処理方法。
【請求項１０】
配送されてきた商品に関連する情報を検証する情報処理装置を制御するコンピュータに実行させるプログラムの記録媒体において、
前記商品とともに配送されてきた情報管理チップにより管理されている秘密鍵に対応する公開鍵の取得を制御する取得制御ステップと、
無作為情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記無作為情報の、近距離無線通信を介して行われる前記情報管理チップに対する送信を制御する送信制御ステップと、
前記送信制御ステップの処理により送信された前記無作為情報に対応するものとして前記情報管理チップにより生成された署名情報の、前記近距離無線通信を介して行われる受信を制御する受信制御ステップと、
前記受信制御ステップの処理により受信された前記署名情報を、前記取得ステップの処理により取得された前記公開鍵を用いて検証する検証ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項１１】
配送されてきた商品に関連する情報を検証する情報処理装置を制御するコンピュータに、
前記商品とともに配送されてきた情報管理チップにより管理されている秘密鍵に対応する公開鍵の取得を制御する取得制御ステップと、
無作為情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記無作為情報の、近距離無線通信を介して行われる前記情報管理チップに対する送信を制御する送信制御ステップと、
前記送信制御ステップの処理により送信された前記無作為情報に対応するものとして前記情報管理チップにより生成された署名情報の、前記近距離無線通信を介して行われる受信を制御する受信制御ステップと、
前記受信制御ステップの処理により受信された前記署名情報を、前記取得ステップの処理により取得された前記公開鍵を用いて検証する検証ステップと
を実行させることを特徴とするプログラム。
【請求項１２】
情報処理装置からの注文に応じて、商品の受注を管理する受注管理装置において、
前記商品の識別情報を含む商品情報、および、前記商品の注文主に関するユーザ情報、並びに、前記情報処理装置により保存されている第１の秘密鍵を用いて生成された、前記商品情報と前記ユーザ情報に対応する第１の署名情報を含む注文情報を、前記情報処理装置から受信する受信手段と、
前記ユーザ情報を認証局に送信し、前記第１の秘密鍵に対応する公開鍵の送信を要求する要求手段と、
前記要求手段による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記第１の署名情報の正当性を検証する検証手段と、
前記検証手段により前記第１の署名情報の正当性が確認されたとき、注文が成立したことを前記情報処理装置に通知する通知手段と
を備えることを特徴とする受注管理装置。
【請求項１３】

第２の秘密鍵を記憶する記憶手段と、
前記記憶手段により記憶されている前記第２の秘密鍵を用いて、前記商品情報、前記ユーザ情報、および、前記受注管理装置の管理者に関する受注者情報に対応する第２の署名情報を生成する生成手段と、
前記商品情報、前記ユーザ情報、前記受注者情報、および、前記生成手段により生成された前記第２の署名情報を含む配送依頼情報を、前記商品の配送を管理する配送管理装置に送信し、前記商品の配送を依頼する配送依頼手段と
をさらに備えることを特徴とする請求項１２に記載の受注管理装置。
【請求項１４】
情報処理装置からの注文に応じて、商品の受注を管理する受注管理装置の受注管理方法において、
前記商品の識別情報を含む商品情報、および、前記商品の注文主に関するユーザ情報、並びに、前記情報処理装置により保存されている秘密鍵を用いて生成された、前記商品情報と前記ユーザ情報に対応する署名情報を含む注文情報を、前記情報処理装置から受信する受信ステップと、
前記ユーザ情報を認証局に送信し、前記秘密鍵に対応する公開鍵の送信を要求する要求ステップと、
前記要求ステップの処理による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記署名情報の正当性を検証する検証ステップと、
前記検証ステップの処理により前記署名情報の正当性が確認されたとき、注文が成立したことを前記情報処理装置に通知する通知ステップと
を含むことを特徴とする受注管理方法。
【請求項１５】
情報処理装置からの注文に応じて、商品の受注を管理する受注管理装置を制御するコンピュータに実行させるプログラムの記録媒体において、
前記商品の識別情報を含む商品情報、および、前記商品の注文主に関するユーザ情報、並びに、前記情報処理装置により保存されている秘密鍵を用いて生成された、前記商品情報と前記ユーザ情報に対応する署名情報を含む注文情報の受信を制御する受信制御ステップと、
前記ユーザ情報の認証局に対する送信を制御し、前記秘密鍵に対応する公開鍵の送信を要求する要求ステップと、
前記要求ステップの処理による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記署名情報の正当性を検証する検証ステップと、
前記検証ステップの処理により前記署名情報の正当性が確認されたとき、注文が成立したことの前記情報処理装置に対する通知を制御する通知制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項１６】
情報処理装置からの注文に応じて、商品の受注を管理する受注管理装置を制御するコンピュータに、
前記商品の識別情報を含む商品情報、および、前記商品の注文主に関するユーザ情報、並びに、前記情報処理装置により保存されている秘密鍵を用いて生成された、前記商品情報と前記ユーザ情報に対応する署名情報を含む注文情報の受信を制御する受信制御ステップと、
前記ユーザ情報の認証局に対する送信を制御し、前記秘密鍵に対応する公開鍵の送信を要求する要求ステップと、
前記要求ステップの処理による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記署名情報の正当性を検証する検証ステップと、
前記検証ステップの処理により前記署名情報の正当性が確認されたとき、注文が成立したことの前記情報処理装置に対する通知を制御する通知制御ステップとを実行させることを特徴とするプログラム。

【請求項１７】
商品の受注を管理する受注管理装置からの依頼に応じて、商品の配送を管理する配送管理装置において、
前記商品の識別情報を含む商品情報、前記商品の注文主に関するユーザ情報、前記受注管理装置の管理者に関する受注者情報、前記受注管理装置により管理される秘密鍵を用いて生成された、前記商品情報、前記ユーザ情報、および前記受注者情報に対応する署名情報を含む前記配送依頼情報を、前記受注管理装置から受信する受信手段と、
前記受注者情報を認証局に送信し、前記秘密鍵に対応する公開鍵の送信を要求する要求手段と、
前記要求手段による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記署名情報の正当性を検証する検証手段と、
前記検証手段により前記署名情報の正当性が確認されたとき、前記商品とともに配送される情報管理チップに、前記商品の配送に関する配送関連情報を記憶させる記憶制御手段とを備えることを特徴とする配送管理装置。
【請求項１８】
前記商品とともに、前記情報管理チップを配送する配送手段をさらに備える
ことを特徴とする請求項１７に記載の配送管理装置。
【請求項１９】
前記配送関連情報には、前記商品情報、前記ユーザ情報、前記受注者情報、および、前記商品の配送を管理する配送管理者に関する配送管理者情報の少なくとも１つの情報が含まれる
ことを特徴とする請求項１７に記載の配送管理装置。
【請求項２０】
前記情報管理チップは、前記商品の表面に貼付されるか、または、前記商品を配送する配送人により保持されることにより、前記商品とともに配送される
ことを特徴とする請求項１７に記載の配送管理装置。
【請求項２１】
商品の受注を管理する受注管理装置からの依頼に応じて、商品の配送を管理する配送管理装置の配送管理方法において、
前記商品の識別情報を含む商品情報、前記商品の注文主に関するユーザ情報、前記受注管理装置の管理者に関する受注者情報、前記受注管理装置により管理される秘密鍵を用いて生成された、前記商品情報、前記ユーザ情報、および前記受注者情報に対応する署名情報を含む前記配送依頼情報を、前記受注管理装置から受信する受信ステップと、
前記受注者情報を認証局に送信し、前記秘密鍵に対応する公開鍵の送信を要求する要求ステップと、
前記要求ステップの処理による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記署名情報の正当性を検証する検証ステップと、
前記検証ステップの処理により前記署名情報の正当性が確認されたとき、前記商品とともに配送される情報管理チップに、前記商品の配送に関する配送関連情報を記憶させる記憶制御ステップと
を含むことを特徴とする配送管理方法。
【請求項２２】
商品の受注を管理する受注管理装置からの依頼に応じて、商品の配送を管理する配送管理装置を制御するコンピュータに実行させるプログラムの記録媒体において、
前記商品の識別情報を含む商品情報、前記商品の注文主に関するユーザ情報、前記受注管理装置の管理者に関する受注者情報、前記受注管理装置により管理される秘密鍵を用いて生成された、前記商品情報、前記ユーザ情報、および前記受注者情報に対応する署名情報を含む前記配送依頼情報の受信を制御する受信制御ステップと、
前記受注者情報の認証局に対する送信を制御し、前記秘密鍵に対応する公開鍵の送信を要求する要求ステップと、

前記要求ステップの処理による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記署名情報の正当性を検証する検証ステップと、
前記検証ステップの処理により前記署名情報の正当性が確認されたとき、前記商品とともに配送される情報管理チップに、前記商品の配送に関する配送関連情報を記憶させる記憶制御ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項２３】
商品の受注を管理する受注管理装置からの依頼に応じて、商品の配送を管理する配送管理装置を制御するコンピュータに、
前記商品の識別情報を含む商品情報、前記商品の注文主に関するユーザ情報、前記受注管理装置の管理者に関する受注者情報、前記受注管理装置により管理される秘密鍵を用いて生成された、前記商品情報、前記ユーザ情報、および前記受注者情報に対応する署名情報を含む前記配送依頼情報の受信を制御する受信制御ステップと、
前記受注者情報の認証局に対する送信を制御し、前記秘密鍵に対応する公開鍵の送信を要求する要求ステップと、
前記要求ステップの処理による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記署名情報の正当性を検証する検証ステップと、
前記検証ステップの処理により前記署名情報の正当性が確認されたとき、前記商品とともに配送される情報管理チップに、前記商品の配送に関する配送関連情報を記憶させる記憶制御ステップと
を実行させることを特徴とするプログラム。
【請求項２４】
商品とともに配送される情報管理チップにおいて、
秘密鍵を記憶する記憶手段と、
前記商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信される無作為情報を受信する受信手段と、
前記記憶手段により記憶されている前記秘密鍵を用いて、前記受信手段により受信された前記無作為情報に対応する第１の署名情報を生成する第１の生成手段と、
前記第１の生成手段により生成された前記第１の署名情報を、前記近距離無線通信を介して前記情報処理装置に送信する第１の送信手段と
を備えることを特徴とする情報管理チップ。
【請求項２５】
前記記憶手段が前記商品の配送に関する配送関連情報をさらに記憶している場合、
前記秘密鍵を用いて前記配送関連情報に対応する第２の署名情報を生成する第２の生成手段と、
前記配送関連情報と、前記第２の生成手段により生成された前記第２の署名情報を、前記近距離無線通信を介して前記情報処理装置に送信する第２の送信手段と
をさらに備えることを特徴とする請求項２４に記載の情報管理チップ。
【請求項２６】
前記記憶手段は、前記商品の識別情報を含む商品情報、前記商品の注文主に関するユーザ情報、前記商品の受注を管理する受注管理装置の管理者に関する受注者情報、および、前記商品の配送を管理する配送管理者に関する配送管理者情報の少なくとも１つを含む情報を前記配送関連情報として記憶する
ことを特徴とする請求項２４に記載の情報管理チップ。
【請求項２７】
商品とともに配送される情報管理チップの情報管理方法において、
秘密鍵を記憶する記憶ステップと、
前記商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信される無作為情報を受信する受信ステップと、

前記記憶ステップの処理により記憶されている前記秘密鍵を用いて、前記受信ステップの処理により受信された前記無作為情報に対応する署名情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記署名情報を、前記近距離無線通信を介して前記情報処理装置に送信する送信ステップと
を含むことを特徴とする情報管理方法。
【請求項２８】
商品とともに配送される情報管理チップを制御するコンピュータに実行させるプログラムの記録媒体において、
秘密鍵の記憶を制御する記憶制御ステップと、
前記商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信される無作為情報の受信を制御する受信制御ステップと、
前記記憶制御ステップの処理により記憶されている前記秘密鍵を用いて、前記受信制御ステップの処理により受信された前記無作為情報に対応する署名情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記署名情報の、前記近距離無線通信を介して行われる前記情報処理装置に対する送信を制御する送信制御ステップと
を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項２９】
商品とともに配送される情報管理チップを制御するコンピュータに、
秘密鍵の記憶を制御する記憶制御ステップと、
前記商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信される無作為情報の受信を制御する受信制御ステップと、
前記記憶制御ステップの処理により記憶されている前記秘密鍵を用いて、前記受信制御ステップの処理により受信された前記無作為情報に対応する署名情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記署名情報の、前記近距離無線通信を介して行われる前記情報処理装置に対する送信を制御する送信制御ステップと
を実行させることを特徴とするプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、検証システムおよび方法、情報処理装置および方法、受注管理装置および方法、配送管理装置および方法、情報管理チップおよび方法、記録媒体、並びにプログラムに関し、特に、配送されてきた荷物の中身や配送元、或いは、配送業者などの荷物の配送に関する様々な情報の正当性を、容易に、かつ確実に確認できるようにする検証システムおよび方法、情報処理装置および方法、受注管理装置および方法、配送管理装置および方法、情報管理チップおよび方法、記録媒体、並びにプログラムに関する。
【０００２】
【従来の技術】
近年、テレビジョン番組により紹介される商品を電話で注文して購入するいわゆるテレフォンショッピングの他に、インターネット等を利用したオンラインショッピングが一般的に普及しつつあり、店舗に出向くことなく、好みの商品を容易に注文できる機会が多くなってきている。
【０００３】
従って、配送業者により配送されてくる商品などの荷物を受け取る機会が多くなってきており、そこへ、配送されてきた荷物に関する悪質な各種の事件がクローズアップされたため、例えば、届けられた商品が本当に自分が注文した商品であり、危険物などではないかどうか、或いは、商品を届けに来た人物が本当に自分が注文した商品を届けに来た配送業者であるかどうかといった不安を感じることなく、商品を安心して受け取ることができる

ような配送システムの重要性が認識されてきている。

【０００４】

例えば、そのような不安を感じることなく商品を受け取ることができる配送システムとして、後述する特許文献１には、製品識別子、署名者識別子、および受領者識別子などのデータと、それに対する署名値（署名データ）が、商品などに貼付されるデータキャリア１（タグ）に記憶されており、その署名を検証することで、製品、署名者、受領者などを確認できるようにするシステムが開示されている。

【０００５】

また、商品に貼付されているタグを利用するものとして、特許文献２には、タグに記憶されている署名を、認証サーバ１０４から発行される公開鍵を用いて検証することにより、商品が本物であるか否かを確認できるようにするシステムが開示されている。

【０００６】

【特許文献１】

特開２０００－３０５９９５号公報（例えば、第１０頁乃至第１２頁）

【特許文献２】

特開２０００－１１１１４号公報（例えば、第２頁乃至第３頁、図１）

【０００７】

【発明が解決しようとする課題】

しかしながら、特許文献１および特許文献２に開示されているシステムにおいては、商品に貼付されているタグ（データキャリア）に、正当な配送元により生成された署名データが保存され、それに基づいて署名データの検証が行われるため、仮に、署名データが第三者に漏洩し、その者が、他のタグに署名データを記憶させて他の商品を配送した場合、受取人は、配送されてきた商品が不正なものであることを見抜くことができないという課題があった。

【０００８】

すなわち、第三者によりタグに記憶された署名データは、正当な配送元により管理されるものと同一のものであるため、商品の受取人が、タグに記憶されている情報を検証した場合であっても、配送されてきた商品が正当なものとして検出されることになる。

【０００９】

本発明はこのような状況に鑑みてなされたものであり、配送されてきた荷物の中身や配送元、或いは、配送業者などの荷物の配送に関する様々な情報の正当性を、容易に、かつ確実に確認できるようにするものである。

【００１０】

【課題を解決するための手段】

本発明の検証システムを構成する情報処理装置は、情報管理チップにより保存されている秘密鍵に対応する公開鍵を取得する取得手段と、無作為情報を生成する無作為情報生成手段と、生成された無作為情報を、近距離無線通信を介して情報管理チップに送信する無作為情報送信手段と、無作為情報に対応するものとして情報管理チップにより生成された署名情報を、近距離無線通信を介して受信する署名情報受信手段と、受信された署名情報を、取得された公開鍵を用いて検証する検証手段とを備えることを特徴とする。

【００１１】

また、本発明の検証システムを構成する情報管理チップは、秘密鍵を記憶する記憶手段と、商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信された無作為情報を受信する無作為情報受信手段と、記憶されている秘密鍵を用いて、受信された無作為情報に対応する署名情報を生成する署名情報生成手段と、生成された署名情報を、近距離無線通信を介して情報処理装置に送信する署名情報送信手段とを備えることを特徴とする。

【００１２】

本発明の検証システムの検証方法を構成する情報処理方法は、情報管理チップにより保存されている秘密鍵に対応する公開鍵を取得する取得ステップと、無作為情報を生成する無

作為情報生成ステップと、生成された無作為情報を、近距離無線通信を介して情報管理チップに送信する無作為情報送信ステップと、無作為情報に対応するものとして情報管理チップにより生成された署名情報を、近距離無線通信を介して受信する署名情報受信ステップと、受信された署名情報を、取得された公開鍵を用いて検証する検証ステップとを含むことを特徴とする。

【００１３】

また、本発明の検証システムの検証方法を構成する情報管理方法は、秘密鍵を記憶する記憶ステップと、商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信された無作為情報を受信する無作為情報受信ステップと、秘密鍵を用いて、受信された無作為情報に対応する署名情報を生成する署名情報生成ステップと、生成された署名情報を、近距離無線通信を介して情報処理装置に送信する署名情報送信ステップとを含むことを特徴とする。

【００１４】

本発明の情報処理装置は、商品とともに配送されてきた情報管理チップにより保存されている第１の秘密鍵に対応する公開鍵を取得する取得手段と、無作為情報を生成する無作為情報生成手段と、生成された無作為情報を、近距離無線通信を介して情報管理チップに送信する送信手段と、無作為情報に対応するものとして情報管理チップにより生成された第１の署名情報を、近距離無線通信を介して受信する署名情報受信手段と、受信された第１の署名情報を、公開鍵を用いて検証する第１の検証手段とを備えることを特徴とする。

【００１５】

第１の秘密鍵を用いて情報管理チップにより生成された、商品の配送に関する配送関連情報に対応する第２の署名情報を、配送関連情報とともに近距離無線通信を介して受信する配送関連情報受信手段と、受信された第２の署名情報を、公開鍵を用いて検証する第２の検証手段とをさらに備えるようにすることができる。このとき、送信手段は、第２の検証手段により第２の署名情報の正当性が確認されたとき、無作為情報を情報管理チップに送信する。

【００１６】

第１の検証手段により第１の署名情報の正当性が確認されたとき、配送関連情報を出力する配送関連情報出力手段をさらに備えるようにすることができる。

【００１７】

第１の検証手段による検証結果を出力する検証結果出力手段をさらに備えるようにすることができる。

【００１８】

第２の秘密鍵を記憶する記憶手段と、記憶されている第２の秘密鍵を用いて、商品の識別情報を含む商品情報、および、商品の注文主に関するユーザ情報に対応する第２の署名情報を生成する署名情報生成手段と、商品情報、ユーザ情報、署名情報生成手段により生成された第２の署名情報を含む注文情報を、商品の受注を管理する受注管理装置に対して送信し、商品を注文する注文手段とをさらに備えるようにすることができる。

【００１９】

商品の注文が受け付けられたことが受注管理装置から通知されてきたとき、第１の秘密鍵に対応する公開鍵の送信を認証局に対して要求する要求手段をさらに備えるようにすることができる。このとき、取得手段は、要求手段による要求に応じて認証局から送信されてきた公開鍵を取得する。

【００２０】

本発明の情報処理装置の情報処理方法は、商品とともに配送されてきた情報管理チップにより管理されている秘密鍵に対応する公開鍵を取得する取得ステップと、無作為情報を生成する生成ステップと、生成された無作為情報を、近距離無線通信を介して情報管理チップに送信する送信ステップと、無作為情報に対応するものとして情報管理チップにより生成された署名情報を、近距離無線通信を介して受信する受信ステップと、受信された署名情報を、取得された公開鍵を用いて検証する検証ステップとを含むことを特徴とする。

【００２１】
本発明の第１の記録媒体は、商品とともに配送されてきた情報管理チップにより管理されている秘密鍵に対応する公開鍵の取得を制御する取得制御ステップと、無作為情報を生成する生成ステップと、生成された無作為情報の、近距離無線通信を介して行われる情報管理チップに対する送信を制御する送信制御ステップと、無作為情報に対応するものとして情報管理チップにより生成された署名情報の、近距離無線通信を介して行われる受信を制御する受信制御ステップと、受信された署名情報を公開鍵を用いて検証する検証ステップとを含むコンピュータが読み取り可能なプログラムが記録されていることを特徴とする。
【００２２】
本発明の第１のプログラムは、配送されてきた商品の正当性を検証する情報処理装置を制御するコンピュータに、商品とともに配送されてきた情報管理チップにより管理されている秘密鍵に対応する公開鍵の取得を制御する取得制御ステップと、無作為情報を生成する生成ステップと、生成された無作為情報の、近距離無線通信を介して行われる情報管理チップに対する送信を制御する送信制御ステップと、無作為情報に対応するものとして情報管理チップにより生成された署名情報の、近距離無線通信を介して行われる受信を制御する受信制御ステップと、受信された署名情報を公開鍵を用いて検証する検証ステップとをコンピュータに実行させることを特徴とする。
【００２３】
本発明の受注管理装置は、商品の識別情報を含む商品情報、および、商品の注文主に関するユーザ情報、並びに、情報処理装置により保存されている第１の秘密鍵を用いて生成された、商品情報とユーザ情報に対応する第１の署名情報を含む注文情報を受信する受信手段と、ユーザ情報を認証局に送信し、第１の秘密鍵に対応する公開鍵の送信を要求する要求手段と、要求手段による要求に応じて認証局から送信されてきた公開鍵を用いて、第１の署名情報の正当性を検証する検証手段と、第１の署名情報の正当性が確認されたとき、注文が成立したことを情報処理装置に通知する通知手段とを備えることを特徴とする。
【００２４】
第２の秘密鍵を記憶する記憶手段と、記憶されている第２の秘密鍵を用いて、商品情報、ユーザ情報、および、受注管理装置の管理者に関する受注者情報に対応する第２の署名情報を生成する生成手段と、商品情報、ユーザ情報、受注者情報、および、生成手段により生成された第２の署名情報を含む配送依頼情報を、商品の配送を管理する配送管理装置に送信し、商品の配送を依頼する配送依頼手段とをさらに備えるようにすることができる。
【００２５】
本発明の受注管理装置の受注管理方法は、商品の識別情報を含む商品情報、および、商品の注文主に関するユーザ情報、並びに、情報処理装置により保存されている秘密鍵を用いて生成された、商品情報とユーザ情報に対応する署名情報を含む注文情報を受信する受信ステップと、ユーザ情報を認証局に送信し、秘密鍵に対応する公開鍵の送信を要求する要求ステップと、要求に応じて認証局から送信されてきた公開鍵を用いて、署名情報の正当性を検証する検証ステップと、署名情報の正当性が確認されたとき、注文が成立したことを情報処理装置に通知する通知ステップとを含むことを特徴とする。
【００２６】
本発明の第２の記録媒体は、商品の識別情報を含む商品情報、および、商品の注文主に関するユーザ情報、並びに、情報処理装置により保存されている秘密鍵を用いて生成された、商品情報とユーザ情報に対応する署名情報を含む注文情報の受信を制御する受信制御ステップと、ユーザ情報の認証局に対する送信を制御し、秘密鍵に対応する公開鍵の送信を要求する要求ステップと、要求に応じて認証局から送信されてきた公開鍵を用いて、署名情報の正当性を検証する検証ステップと、署名情報の正当性が確認されたとき、注文が成立したことの情報処理装置に対する通知を制御する通知制御ステップとを含むコンピュータが読み取り可能なプログラムが記録されていることを特徴とする。
【００２７】
本発明の第２のプログラムは、商品の識別情報を含む商品情報、および、商品の注文主に

関するユーザ情報、並びに、情報処理装置により保存されている秘密鍵を用いて生成された、商品情報とユーザ情報に対応する署名情報を含む注文情報の受信を制御する受信制御ステップと、ユーザ情報の認証局に対する送信を制御し、秘密鍵に対応する公開鍵の送信を要求する要求ステップと、要求に応じて認証局から送信されてきた公開鍵を用いて、署名情報の正当性を検証する検証ステップと、署名情報の正当性が確認されたとき、注文が成立したことの情報処理装置に対する通知を制御する通知制御ステップとコンピュータに実行させることを特徴とする。

【００２８】

本発明の配送管理装置は、商品の識別情報を含む商品情報、商品の注文主に関するユーザ情報、受注管理装置の管理者に関する受注者情報、受注管理装置により保存される秘密鍵を用いて生成された、商品情報、ユーザ情報、および受注者情報に対応する署名情報を含む配送依頼情報を受信する受信手段と、受注者情報を認証局に送信し、秘密鍵に対応する公開鍵の送信を要求する要求手段と、要求に応じて認証局から送信されてきた公開鍵を用いて、署名情報の正当性を検証する検証手段と、署名情報の正当性が確認されたとき、商品とともに配送される情報管理チップに、商品の配送に関する配送関連情報を記憶させる記憶制御手段とを備えることを特徴とする。

【００２９】

商品とともに、情報管理チップを配送する配送手段をさらに備えるようにすることができる。

【００３０】

配送関連情報には、商品情報、ユーザ情報、受注者情報、および、商品の配送を管理する配送管理者に関する配送管理者情報の少なくとも１つの情報が含まれるようにすることができる。

【００３１】

情報管理チップは、商品の表面に貼付されるか、または、商品を配送する配送人により保持されることにより、商品とともに配送されるようにすることができる。

【００３２】

本発明の配送管理装置の配送管理方法は、商品の識別情報を含む商品情報、商品の注文主に関するユーザ情報、受注管理装置の管理者に関する受注者情報、受注管理装置により保存される秘密鍵を用いて生成された、商品情報、ユーザ情報、および受注者情報に対応する署名情報を含む配送依頼情報を受信する受信ステップと、受注者情報を認証局に送信し、秘密鍵に対応する公開鍵の送信を要求する要求ステップと、要求に応じて認証局から送信されてきた公開鍵を用いて、署名情報の正当性を検証する検証ステップと、署名情報の正当性が確認されたとき、商品とともに配送される情報管理チップに、商品の配送に関する配送関連情報を記憶させる記憶制御ステップとを含むことを特徴とする。

【００３３】

本発明の第３の記録媒体は、商品の識別情報を含む商品情報、商品の注文主に関するユーザ情報、受注管理装置の管理者に関する受注者情報、受注管理装置により保存される秘密鍵を用いて生成された、商品情報、ユーザ情報、および受注者情報に対応する署名情報を含む配送依頼情報の受信を制御する受信制御ステップと、受注者情報の認証局に対する送信を制御し、秘密鍵に対応する公開鍵の送信を要求する要求ステップと、要求に応じて認証局から送信されてきた公開鍵を用いて、署名情報の正当性を検証する検証ステップと、署名情報の正当性が確認されたとき、商品とともに配送される情報管理チップに、商品の配送に関する配送関連情報を記憶させる記憶制御ステップとを含むコンピュータが読み取り可能なプログラムが記録されていることを特徴とする。

【００３４】

本発明の第３のプログラムは、商品の識別情報を含む商品情報、商品の注文主に関するユーザ情報、受注管理装置の管理者に関する受注者情報、受注管理装置により保存される秘密鍵を用いて生成された、商品情報、ユーザ情報、および受注者情報に対応する署名情報を含む配送依頼情報の受信を制御する受信制御ステップと、受注者情報の認証局に対する

送信を制御し、秘密鍵に対応する公開鍵の送信を要求する要求ステップと、要求に応じて認証局から送信されてきた公開鍵を用いて、署名情報の正当性を検証する検証ステップと、署名情報の正当性が確認されたとき、商品とともに配送される情報管理チップに、商品の配送に関する配送関連情報を記憶させる記憶制御ステップとをコンピュータに実行させることを特徴とする。

【００３５】

本発明の情報管理チップは、秘密鍵を記憶する記憶手段と、商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信される無作為情報を受信する受信手段と、秘密鍵を用いて、無作為情報に対応する第１の署名情報を生成する第１の生成手段と、生成された第１の署名情報を、近距離無線通信を介して情報処理装置に送信する第１の送信手段とを備えることを特徴とする。

【００３６】

記憶手段が商品の配送に関する配送関連情報をさらに記憶している場合、秘密鍵を用いて配送関連情報に対応する第２の署名情報を生成する第２の生成手段と、配送関連情報と、第２の生成手段により生成された第２の署名情報を、近距離無線通信を介して情報処理装置に送信する第２の送信手段とをさらに備えるようにすることができる。

【００３７】

記憶手段は、商品の識別情報を含む商品情報、商品の注文主に関するユーザ情報、商品の受注を管理する受注管理装置の管理者に関する受注者情報、および、商品の配送を管理する配送管理者に関する配送管理者情報の少なくとも１つを含む情報を配送関連情報として記憶するようにすることができる。

【００３８】

本発明の情報管理チップの情報管理方法は、秘密鍵を記憶する記憶ステップと、商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信される無作為情報を受信する受信ステップと、秘密鍵を用いて、受信された無作為情報に対応する署名情報を生成する生成ステップと、生成された署名情報を、近距離無線通信を介して情報処理装置に送信する送信ステップとを含むことを特徴とする。

【００３９】

本発明の第４の記録媒体は、秘密鍵の記憶を制御する記憶制御ステップと、商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信される無作為情報の受信を制御する受信制御ステップと、秘密鍵を用いて、受信された無作為情報に対応する署名情報を生成する生成ステップと、生成された署名情報の、近距離無線通信を介して行われる情報処理装置に対する送信を制御する送信制御ステップとを含むコンピュータが読み取り可能なプログラムが記録されていることを特徴とする。

【００４０】

本発明の第４のプログラムは、秘密鍵の記憶を制御する記憶制御ステップと、商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信される無作為情報の受信を制御する受信制御ステップと、秘密鍵を用いて、受信された無作為情報に対応する署名情報を生成する生成ステップと、生成された署名情報の、近距離無線通信を介して行われる情報処理装置に対する送信を制御する送信制御ステップとをコンピュータに実行させることを特徴とする。

【００４１】

本発明の検証システムおよび方法においては、情報管理チップにより管理されている秘密鍵に対応する公開鍵が取得され、無作為情報が生成され、生成された無作為情報が、近距離無線通信を介して情報管理チップに送信される。また、無作為情報に対応するものとして情報管理チップにより生成された署名情報が、近距離無線通信を介して受信され、取得された公開鍵を用いて検証される。

【００４２】

さらに、本発明の検証システムにおいては、秘密鍵が記憶され、商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信された無作為情報が受信され、記

憶されている秘密鍵を用いて、受信された無作為情報に対応する署名情報が生成され、生成された署名情報が、近距離無線通信を介して情報処理装置に送信される。

【００４３】

本発明の情報処理装置および方法、並びに、プログラムにおいては、商品とともに配送されてきた情報管理チップにより保存されている秘密鍵に対応する公開鍵が取得され、無作為情報が生成される。また、生成された無作為情報が、近距離無線通信を介して情報管理チップに送信され、情報管理チップにより無作為情報に対応するものとして生成された署名情報が、近距離無線通信を介して受信され、公開鍵を用いて検証される。

【００４４】

本発明の受注管理装置および方法、並びに、プログラムにおいては、商品の識別情報を含む商品情報、および、商品の注文主に関するユーザ情報、並びに、情報処理装置により保存されている第１の秘密鍵を用いて生成された、商品情報とユーザ情報に対応する第１の署名情報を含む注文情報が受信され、ユーザ情報が認証局に送信され、第１の秘密鍵に対応する公開鍵の送信が要求される。また、要求に応じて認証局から送信されてきた公開鍵を用いて、第１の署名情報の正当性が検証され、第１の署名情報の正当性が確認されたとき、注文が成立したことが情報処理装置に通知される。

【００４５】

本発明の配送管理装置および方法、並びに、プログラムにおいては、商品の識別情報を含む商品情報、商品の注文主に関するユーザ情報、受注管理装置の管理者に関する受注者情報、受注管理装置により保存される秘密鍵を用いて生成された、商品情報、ユーザ情報、および受注者情報に対応する署名情報を含む配送依頼情報が受信され、受注者情報を認証局に送信が、秘密鍵に対応する公開鍵の送信が要求される。また、要求に応じて認証局から送信されてきた公開鍵を用いて、署名情報の正当性が検証され、署名情報の正当性が確認されたとき、商品とともに配送される情報管理チップに、商品の配送に関する配送関連情報が記憶される。

【００４６】

本発明の情報管理チップおよび方法、並びに、プログラムにおいては、秘密鍵が記憶され、商品の受取人により操作される情報処理装置から、近距離無線通信を介して送信される無作為情報が受信される。また、秘密鍵を用いて、無作為情報に対応する第１の署名情報が生成され、生成された第１の署名情報が、近距離無線通信を介して情報処理装置に送信される。

【００４７】

【発明の実施の形態】

図１は、本発明を適用した商品配送システムの構成例を示す図である。

【００４８】

本発明を適用した商品配送システムは、基本的に、ユーザ端末１（情報処理装置）、メーカ端末２、配送業者端末３、および認証局（ＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ Ａｕｔｈｏｒｉｔｙ））４から構成され、これらの間における各種の情報の送受信は、インターネットなどのネットワークを介して行われる。

【００４９】

ユーザ端末１は、商品の需要者であるユーザにより操作され、商品の販売を行っているショッピングサイト（Ｗｅｂサイト）にアクセスすることが指示されたとき、その指示に応じてアクセスし、ダウンロードされたデータに基づいてショッピングサイトの画面を表示する。また、ユーザ端末１は、ショッピングサイトにおいて販売されている商品を注文することが指示されたとき、自分自身が管理している秘密鍵を用いて、購入する商品に関する商品情報、および、注文主であるユーザに関するユーザ情報に対応する署名情報を生成し、生成した署名情報を、商品情報とユーザ情報とともに注文情報としてメーカ端末２に送信する。この例においては、メーカ端末２によりショッピングサイトが管理され、商品の受注が管理されている。

【００５０】

注文情報に含まれ、メーカ端末２に送信される商品情報には、例えば、注文する商品を識別する情報、注文する個数、価格などを表す情報が含まれ、一方、ユーザ情報には、配送先を指定する情報、注文主の氏名、電話番号、支払い方法などを表す情報が含まれる。

【００５１】

メーカ端末２は、ユーザ端末１から注文情報が送信されてきたとき、注文情報に含まれているユーザ情報を認証局に送信し、ユーザにより予め登録されている公開鍵（ユーザ端末１により管理されている秘密鍵に対応する公開鍵）の送信を要求する。その要求に応じて公開鍵が送信されてきたとき、メーカ端末２は、公開鍵を利用して、ユーザ端末１から送信されてきた注文情報に含まれる署名情報を検証し、注文情報（ユーザ情報および商品情報）に対して改竄や切除が第三者により施されていないか否か、すなわち、情報が正当なものであるか否かを確認する。

【００５２】

なお、図１においては、認証局４との間で行われる公開鍵の要求と、それに対する公開鍵の送信は一点鎖線により表され、ユーザ端末１、メーカ端末２、および配送業者端末３の各端末間における情報の送受信は実線により表されている。

【００５３】

メーカ端末２は、署名情報の検証の結果、ユーザ端末１から送信されてきた注文情報の正当性が確認できたと判定した場合、注文を受け付けたことをユーザ端末１に通知すべく、自分自身が管理する秘密鍵を用いて、商品を配送する配送業者に関する情報である配送業者情報に対応する署名情報を生成し、生成した署名情報と配送業者情報を含む配送業者通知情報をユーザ端末１に送信する。

【００５４】

例えば、配送業者情報には、配送業者の名称や連絡先、ユーザにより指定された配送先の近隣にある営業所の名称、配送時間帯などを表す情報が含まれる。

【００５５】

配送業者通知情報を受信したユーザ端末１は、認証局４に対して、メーカ端末２の管理者（メーカ）により予め登録されている公開鍵と、配送業者端末３の管理者（配送業者）により予め登録されている公開鍵の送信を要求し、送信されてきた公開鍵（メーカの公開鍵）を用いて、メーカ端末２から送信されてきた配送業者通知情報の検証を行う。

【００５６】

検証の結果、送信されてきた配送業者通知情報が正当なものであると判定された場合、ユーザ端末１は、認証局４から取得した配送業者の公開鍵を、内蔵する記憶部に保存する。後述するように、保存された配送業者の公開鍵は、配送業者により商品（商品６）とともに配送されてくるＰＫＩ（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）チップ５との間で行われる、署名情報の検証処理において利用される。

【００５７】

また、メーカ端末２は、配送業者通知情報をユーザ端末１に送信するとともに、ユーザにより注文された商品の配送を依頼すべく、配送業者端末３に対して配送依頼情報を送信する。

【００５８】

配送依頼情報には、商品情報、ユーザ情報、および、メーカの名称や住所などを表す情報を含むメーカ情報の他に、メーカ端末２により管理されている秘密鍵を用いて生成された、商品情報、ユーザ情報、およびメーカ情報に対応する署名情報が含まれている。

【００５９】

配送業者端末３は、メーカ端末２から配送依頼情報が送信されてきたとき、その正当性を確認すべく、認証局４に対してメーカにより予め登録されている公開鍵の送信を要求し、要求に応じて送信されてきた公開鍵を利用して、配送依頼情報に含まれる署名情報の検証を行う。

【００６０】

配送依頼情報に対して改竄等が施されていないことが確認できたとき、配送業者端末３は

、商品６（ユーザ端末１のユーザにより注文された商品）を配送する配送人を選択し、その配送人が有するＩＤカードに配設されるＰＫＩチップ５に、配送依頼情報に含まれる商品情報、ユーザ情報、およびメーカ情報などの配送に関連する情報を記憶させる。

【００６１】

配送人は、指定された配送先に商品６を配送し、応対する受取人としてのユーザに対して、自分自身のＩＤカードを提示する。ユーザは、ユーザ端末１に設けられているリーダライタを、提示されたＩＤカード（ＰＫＩチップ５）に近接させ、認証局４から予め取得しておいた配送業者の公開鍵を用いて、ＰＫＩチップ５に記憶されている情報の正当性、すなわち、商品６の正当性の確認を行う。

【００６２】

ユーザ端末１によりＰＫＩチップ５との間で行われる検証の結果は、ユーザ端末１に出力され、例えば、正当性が確認できなかったとき、商品の引き取りを中止することを促すメッセージが表示され、一方、情報の正当性が確認できたとき、ＰＫＩチップ５に記憶されている商品情報、メーカ情報、およびユーザ情報に基づいて、それぞれ、荷物の中身を表す情報、配送元を表す情報、および、注文主であるユーザ自身を表す情報が表示される。また、ユーザ端末１の表示部には、商品を安全に引き取ることができることを通知するメッセージなども表示される。

【００６３】

以上のように、各種の情報の送受信が、その都度、送信元において生成された署名情報を認証局４から発行される公開鍵を用いて検証する、いわゆるＰＫＩの検証を経て行われるため、第三者により改竄や切除等が施された不正な情報がＰＫＩチップ５に記憶されることを防止することができる。

【００６４】

従って、商品とともに配送されてくるＰＫＩチップ５には、信頼性のある情報が記憶されることとなるため、ユーザは、ユーザ端末１に出力される、ＰＫＩチップ５との間で行われる検証結果を信頼し、安心して商品を受け取ることできる。例えば、ＰＫＩチップ５に記憶されている情報が信頼できないものである場合、ユーザ端末１に表示される検証結果が正しくない場合が起こりうるが、そのようなことを抑制することができる。

【００６５】

また、後述するように、ユーザ端末１とＰＫＩチップ５との間で行われる署名情報の検証は、そのときに選択された乱数に基づいて生成された署名情報によっても行われるため、例えば、商品を配送する段階で、配送業者端末３によりＰＫＩチップ５に記憶された署名情報のみに基づいて検証を行う場合に較べて、より確実な検証結果を得ることができる。

【００６６】

以上においては、ＰＫＩチップ５は、商品６とは別に、配送人が提示するＩＤカードに配設されているとしたが、例えば、商品６の表面の所定の位置に貼付されているなど、様々な形態でユーザに提供されるようにすることができる。

【００６７】

次に、図１のユーザ端末１、メーカ端末２、配送業者端末３、認証局４、およびＰＫＩチップ５の各構成について説明する。

【００６８】

図２は、図１のユーザ端末１の構成例を示すブロック図である。

【００６９】

ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１１は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１２に記憶されているプログラム、または、記憶部１８からＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１３にロードされたプログラムに従って各種の処理を実行する。ＲＡＭ１３にはまた、ＣＰＵ１１が各種の処理を実行する上において必要なデータなどが適宜記憶される。

【００７０】

ＣＰＵ１１、ＲＯＭ１２、およびＲＡＭ１３は、バス１４を介して相互に接続されている

。このバス１４にはまた、入出力インタフェース１５も接続されている。

【００７１】

入出力インタフェース１５には、キーボード、マウスなどよりなる入力部１６、ＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ），ＬＣＤ（Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）などよりなるディスプレイ、並びにスピーカなどよりなる出力部１７、ハードディスクなどより構成される記憶部１８、モデムなどより構成される通信部１９が接続されている。通信部１９は、ネットワークを介して、メーカ端末２および認証局４との間で各種の通信を行う。

【００７２】

リーダライタ２０は、ＣＰＵ１１からの制御に基づいて、図示せぬアンテナから電磁波を輻射し、電磁波を受信することで生じた誘起電力を利用して駆動するＰＫＩチップ５が近傍（電磁波が届く範囲）で検出されたとき、ＰＫＩチップ５との間で各種の情報の送受信を行う。

【００７３】

入出力インタフェース１５にはまた、必要に応じてドライブ２１が接続され、磁気ディスク２２、光ディスク２３、光磁気ディスク２４、或いは半導体メモリ２５などが適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じて記憶部１８にインストールされる。

【００７４】

なお、記憶部１８には、一点鎖線で示されるように、ユーザの秘密鍵（Ｋ$_{s}$$_{,}$$_{,}$$_{,}$（ユーザ））が記憶されている。ユーザは、図１に示される配送システムを利用するにあたって、認証局４に公開鍵の発行を依頼し、その公開鍵に対応する秘密鍵をユーザ端末１に保存させている。

【００７５】

図３は、図１のメーカ端末２の構成例を示すブロック図である。

【００７６】

図３に示されるように、メーカ端末２は、リーダライタが設けられていない点を除いて、図２に示されるユーザ端末１と基本的に同様の構成を有している。上述したものと重複する部分については、その詳細な説明を適宜省略する。

【００７７】

メーカ端末２は、メーカの管理者により管理され、その記憶部３８には、一点鎖線で示されるように、メーカの秘密鍵（Ｋ$_{s}$$_{,}$$_{,}$$_{,}$（メーカ））が記憶されている。メーカは、図１に示される配送システムを利用して受注し、商品を配送するにあたって、認証局４に公開鍵の発行を依頼し、その公開鍵に対応する秘密鍵をメーカ端末２に保存させている。

【００７８】

図４は、図１の配送業者端末３の構成例を示すブロック図である。

【００７９】

配送業者端末３も基本的に図２に示されるユーザ端末１と同様の構成を有しているため、重複する部分については詳細な説明を適宜省略する。

【００８０】

配送業者端末３の記憶部５８には、一点鎖線で示されるように、配送業者の秘密鍵（Ｋ$_{s}$$_{,}$$_{,}$$_{,}$（配送業者））が記憶されている。配送業者は、図１に示される配送システムにより配送の依頼をメーカから受け付け、依頼に従って商品を配送する前に、認証局４に公開鍵の発行を依頼し、その公開鍵に対応する秘密鍵を配送業者端末３に保存させている。

【００８１】

リーダライタ６０は、ＣＰＵ５１からの制御に基づいて電磁波を輻射し、例えば、商品とともに配送先に配送されるＰＫＩチップ５が近接されたとき、輻射する電磁波を介して、商品情報、メーカ情報、およびユーザ情報をＰＫＩチップ５に送信し、記憶させる。

【００８２】

図５は、ＰＫＩチップ５の構成例を示すブロック図である。

【００８３】
ＣＰＵ８１は、電源供給部８５から供給される電力により駆動し、ＲＯＭに記憶されている制御プログラムをＲＡＭ（いずれも図示せず）に展開し、展開した制御プログラムに従って、ＰＫＩチップ５全体の動作を制御する。例えば、ＣＰＵ８１は、配送業者端末３のリーダライタ６０から、商品情報、メーカ情報、およびユーザ情報を記憶することが指示されたとき（通信部８２を介して商品情報、メーカ情報、およびユーザ情報が供給されてきたとき）、それらの情報をメモリ８４に保存させる。
【００８４】
通信部８２は、ループアンテナにおいて受信された変調波（電磁波）を包絡線検波して復調し、復調後のデータをＣＰＵ８１に出力する。また、通信部８２は、署名情報などをユーザ端末１のリーダライタ２０に送信する場合、ＣＰＵ８１から供給されるデータに対応して、例えば、所定のスイッチング素子をオン／オフさせ、スイッチング素子がオン状態であるときだけ、所定の負荷をループアンテナに並列に接続させることにより負荷を変動させ、その変動により、リーダライタ２０からの電磁波を変調し、その変調成分をリーダライタ２０に送信する。
【００８５】
なお、通信部８２からリーダライタ２０に送信される情報は、演算部８３において、所定の方式に従って適宜暗号化が施される。
【００８６】
演算部８３は、ＣＰＵ８１からの制御に基づいて署名情報を生成し、例えば、所定の桁数の乱数がユーザ端末１のリーダライタ２０から送信されてきたとき、それに対応する署名情報を、メモリ８４に保存されている秘密鍵を用いて生成する。生成された署名情報は、通信部８２を介してリーダライタ２０に送信される。
【００８７】
メモリ８４は、不揮発性のメモリから構成され、例えば、配送業者が管理する秘密鍵（K_{pri}（配送業者））が保存される。メモリ８４に記憶されている秘密鍵（K_{pri}（配送業者））は、ＣＰＵ８１を介して演算部８３に供給され、署名情報の生成において利用される。上述したように、メモリ８４に保存されている秘密鍵に対応する公開鍵が認証局４から配布されている。
【００８８】
電源供給部８５は、ループアンテナにおいて励起された交流磁界を整流し、それを安定化した後、ＰＫＩチップ５の各部に直流電源として供給する。リーダライタ２０またはリーダライタ６０から輻射される電磁波の電力は、ＰＫＩチップ５に必要な電力を賄う磁界を発生させるように調整されている。
【００８９】
なお、「ＰＫＩチップ」とは、説明の便宜上用いたものであり、例えば、ＲＳＡ暗号系や楕円曲線暗号系などを利用した公開鍵暗号システムにおいて、署名の生成や、その検証を、ハードウエアにより行うＩＣ（情報管理チップ）を表している。
【００９０】
図６は、認証局４の構成例を示すブロック図である。
【００９１】
認証局４も、上述したユーザ端末１、メーカ端末２、および配送業者端末３と基本的に同様の構成を有している。
【００９２】
記憶部１０８には、ユーザ端末１により管理されている秘密鍵に対応する公開鍵（K_{pub}（ユーザ））、メーカ端末２により管理されている秘密鍵に対応する公開鍵（K_{pub}（メーカ））、配送業者端末３により管理されている秘密鍵に対応する公開鍵（K_{pub}（配送業者））が保存されている。
【００９３】
図１の配送システムにおいては、ＣＰＵ１０１は、ユーザ端末１からの要求に応じて、メ

ーカにより登録されている公開鍵と、配送業者により登録されている公開鍵を通信部１０９を介して提供し、メーカ端末２からの要求に応じて、ユーザにより登録されている公開鍵を提供する。また、ＣＰＵ１０１は、配送業者端末３からの要求に応じて、メーカにより登録されている公開鍵を通信部１０９を介して提供する。

【００９４】

次に、図１の配送システムの動作についてフローチャートを参照して説明する。

【００９５】

始めに、図７のフローチャートを参照して、メーカ端末２に対して商品を注文するユーザ端末１の注文処理について説明する。

【００９６】

ステップＳ１において、ユーザ端末１のＣＰＵ１１は、ユーザからの指示に従って、メーカが管理するショッピングサイトにアクセスし、ショッピングサイトの画面を、出力部１７を構成する表示部に表示させる。

【００９７】

ＣＰＵ１１は、ステップＳ２において、入力部１６からの出力に基づいて、ユーザにより商品の注文が指示されたか否かを判定し、注文されたと判定するまで待機する。例えば、商品が注文されずに、ショッピングサイトへのアクセスを終了することがユーザにより指示されたとき、図７に示される処理は終了される。

【００９８】

ステップＳ２において、ＣＰＵ１１は、ショッピングサイトにおいて販売されている商品の中から、所定の商品の注文が指示されたと判定した場合、ステップＳ３に進み、記憶部１８に記憶されている秘密鍵（K_{u1}（ユーザ））を用いて、商品情報およびユーザ情報に対応する署名情報を生成する。

【００９９】

具体的には、ＣＰＵ１１は、注文が指示された商品の識別情報と、注文する個数などを表す情報を含む商品情報、および、ユーザの氏名、配送先、電話番号、メールアドレス、支払い方法などを表す情報を含むユーザ情報を、ユーザからの入力に基づいて取得し、取得した商品情報およびユーザ情報にハッシュ関数を適用する。また、ＣＰＵ１１は、ハッシュ関数を適用して得られたメッセージダイジェストを、秘密鍵を利用して暗号化し、得られた暗号化データを署名情報とする。

【０１００】

ＣＰＵ１１は、ステップＳ４において、通信部１９を制御し、商品情報、ユーザ情報、および、ステップＳ３で生成した署名情報を含む注文情報を、ネットワークを介して商品の受注を管理するメーカ端末２に送信する。

【０１０１】

次に、図８のフローチャートを参照して、図７の処理に対応して実行される、メーカ端末２の受注処理について説明する。

【０１０２】

ステップＳ１１において、メーカ端末２のＣＰＵ３１は、通信部３９からの出力に基づいて、ユーザ端末１から注文情報が送信されてきたか否かを判定し、注文情報が送信されてきたと判定するまで待機する。

【０１０３】

ＣＰＵ３１は、ステップＳ１１において、注文情報が送信されてきたと判定した場合、ステップＳ１２に進み、通信部３９を制御して注文情報を受信する。ＣＰＵ３１は、ステップＳ１３において、注文情報に含まれるユーザ情報を認証局４に送信し、ユーザ端末１により管理されている秘密鍵に対応する公開鍵（証明書）の送信を要求する。

【０１０４】

メーカ端末２と認証局４との間では、必要に応じて、公開鍵の発行を要求するメーカの確認が行われ、メーカの確認が完了したとき、ユーザ端末１により管理されている秘密鍵（K_{u1}（ユーザ））に対応する公開鍵（K_{u2}（ユーザ））を含む証明書が送信され

てくる。

【０１０５】

ＣＰＵ３１は、ステップＳ１４において、通信部３９からの出力に基づいて、認証局４から証明書が送信されてきたか否かを判定し、送信されてきたと判定するまで待機する。

【０１０６】

ステップＳ１４において、ＣＰＵ３１は、認証局４から公開鍵を含む証明書が送信されてきたと判定した場合、ステップＳ１５に進み、それを受信し（取得し）、ステップＳ１６に進む。

【０１０７】

ステップＳ１６において、ＣＰＵ３１は、注文情報に含まれる商品情報およびユーザ情報にハッシュ関数を適用し、メッセージダイジェスト（ＭＤ）を生成する。また、ＣＰＵ３１は、ステップＳ１７において、証明書に含まれる公開鍵を用いて、注文情報に含まれる署名情報（図７のステップＳ３において生成された署名情報）を復号し、メッセージダイジェストを生成する。

【０１０８】

ステップＳ１８において、ＣＰＵ３１は、ステップＳ１６で生成したメッセージダイジェストと、ステップＳ１７で生成したメッセージダイジェストとを比較し、それらが一致するか否かを判定する。この判定により、２つのメッセージダイジェストが一致しない、すなわち異なっていると判定された場合、それは、注文情報およびユーザ情報に対して第三者により改竄等が施されたおそれがあることを表しており、一方、２つのメッセージダイジェストが一致すると判定された場合、ユーザ情報および商品情報には改竄等が施されておらず、信頼できる情報であることを表している。

【０１０９】

従って、ＣＰＵ３１は、ステップＳ１８において、ステップＳ１６で生成したメッセージダイジェストと、ステップＳ１７で生成したメッセージダイジェストとが一致しないと判定した場合、ステップＳ１９に進み、注文を受け付けることができないこと通知するメッセージをユーザ端末１に送信し、その後、処理を終了させる。

【０１１０】

一方、ステップＳ１８において、ＣＰＵ３１は、ステップＳ１６で生成したメッセージダイジェストと、ステップＳ１７で生成したメッセージダイジェストが一致すると判定した場合、注文が信頼できるものであるため、ステップＳ２０に進み、配送業者に関する情報をユーザに通知すべく、記憶部３８に記憶されている秘密鍵（Ｋ$_{メーカ}^{-1}$）を用いて配送業者情報に対応する署名情報を生成する。

【０１１１】

配送業者情報には、配送業者の名称、指定された配送先の近隣にある営業所、配送日時などを表す情報が含まれており、ユーザ端末１から送信されてきた注文情報、および、記憶部３８に構築されている配送業者のデータベースにおいて管理されている情報に基づいて生成される。具体的には、ＣＰＵ３１は、ステップＳ２０において、配送業者情報にハッシュ関数を適用し、生成されたメッセージダイジェストを秘密鍵（Ｋ$_{メーカ}^{-1}$）により暗号化し、得られた暗号化データを署名情報とする。

【０１１２】

ＣＰＵ３１は、ステップＳ２１において、配送業者情報と、ステップＳ２０で生成した署名情報を含む配送業者通知情報を、通信部３９を介してユーザ端末１に送信し、注文を受け付けたことを通知する。

【０１１３】

以上の処理により、ユーザ端末１において生成された署名情報に基づいて、ユーザからメーカに対して送信された注文情報が正当なものであると判定された場合にのみ、注文情報が受け付けられることになる。すなわち、不正な商品の注文が抑制されることになる。

【０１１４】

次に、図９のフローチャートを参照して、図８の処理によりメーカ端末２から送信されて

くる配送業者通知情報が正当であるか否かを検証するユーザ端末１の処理について説明する。

【０１１５】

ステップＳ３１において、ユーザ端末１のＣＰＵ１１は、注文が受け付けられたことがメーカ端末２から通知されてきたか否かを判定する。上述したように、メーカ端末２においては、注文情報が信頼できる情報であるか否かが判定され、信頼できる情報であると判定された場合、ユーザ端末１に対して、注文が受け付けられたことが通知されてくる（図８のステップＳ２１）。

【０１１６】

ＣＰＵ１１は、ステップＳ３１において、注文が受け付けられたことが通知されてこない、すなわち、注文情報が不正なものであるとメーカ端末２により判定され、注文を受け付けることができないことが通知されてきたと判定した場合、ステップＳ３２に進み、エラー処理を行う。

【０１１７】

例えば、エラー処理として、メーカ端末２から送信されてきた、注文を受け付けることができない旨を通知するメッセージが出力部１７に表示され、ユーザに提示される。その後、処理は終了される。

【０１１８】

一方、ステップＳ３１において、商品が受け付けられたことが通知されてきたと判定した場合、ＣＰＵ１１は、ステップＳ３３に進み、通信部１９を制御し、配送業者通知情報を受信する。

【０１１９】

ＣＰＵ１１は、ステップＳ３４において、メーカ情報と配送業者情報を認証局４に送信し、メーカ端末２により管理されている秘密鍵（K_{priMK}（メーカ））に対応する公開鍵（K_{pubMK}（メーカ））と、配送業者端末３により管理されている秘密鍵（K_{priSC}（配送業者））に対応する公開鍵（K_{pubSC}（配送業者））の送信を要求する。

【０１２０】

この要求に応じて、認証局４においては、公開鍵（K_{pubMK}（メーカ）、K_{pubSC}（配送業者））が記憶部１０８に構築されているデータベースから読み出され、それらを含む証明書がユーザ端末１に対して送信される。

【０１２１】

ＣＰＵ１１は、ステップＳ３５において、証明書が送信されてきたと判定するまで待機し、証明書が送信されてきたと判定した場合、ステップＳ３６に進み、それを受信する。

【０１２２】

ステップＳ３７において、ＣＰＵ１１は、メーカ端末２から送信されてきた配送業者通知情報に含まれる配送業者情報が正当なものであるか否かを検証すべく、配送業者情報にハッシュ関数を適用し、メッセージダイジェストを生成する。また、ＣＰＵ１１は、ステップＳ３８において、証明書に含まれる公開鍵（K_{pubMK}（メーカ））を用いて署名情報（メーカ端末２において、秘密鍵（K_{priMK}（メーカ））により暗号化され、生成された署名情報）を復号し、メッセージダイジェストを生成する。

【０１２３】

ＣＰＵ１１は、ステップＳ３９において、ステップＳ３７で生成したメッセージダイジェストと、ステップＳ３８で生成したメッセージダイジェストを比較し、それらのメッセージダイジェストが一致するか否かを判定する。

【０１２４】

ステップＳ３９において、ステップＳ３７で生成したメッセージダイジェストと、ステップＳ３８で生成したメッセージダイジェストが一致しないと判定された場合、それは、配送業者情報が信頼できない情報であることを表しているため、ＣＰＵ１１は、ステップＳ３２に進み、エラー処理を実行する。例えば、ＣＰＵ１１は、ステップＳ３２において、配送業者情報が不正な情報であるおそれがあるため、商品の注文を中止することを通知す

るメッセージを表示する。

【０１２５】

一方、ステップＳ３９において、ステップＳ３７で生成したメッセージダイジェストと、ステップＳ３８で生成したメッセージダイジェストが一致すると判定された場合、それは、メーカ端末２から送信されてきた配送業者通知情報が信頼できる情報であることを表しているため、ＣＰＵ１１は、ステップＳ４０に進み、商品を配送してくる予定の配送業者に関する情報（配送業者名、配送日時などの情報）をユーザに提示するとともに、認証局４から送信されてきた公開鍵（Ｋｐｕｂ（配送業者））を記憶部１８に保存させる。

【０１２６】

記憶部１８に保存された公開鍵（Ｋｐｕｂ（配送業者））は、商品が実際に配送されてきたとき、商品とともに配送されてくるＰＫＩチップ５との間で行われる検証処理において利用される。

【０１２７】

以上のように、メーカ端末２から、商品を配送する配送業者に関する情報として通知されてきた情報を、メーカ端末２により管理されている秘密鍵に対応する公開鍵を利用して検証し、正当なものであることが検出された場合にのみ、注文処理を続行するようにしたため、ユーザに対して提示された配送業者の名称や配送日時などの情報は、第三者により改竄等が施されていない、信頼できる情報となる。すなわち、ユーザは、メーカにより正式に依頼された配送業者から、商品が配送されることを確認することができる。

【０１２８】

次に、図１０のフローチャートを参照して、配送業者に対して商品の配送を依頼するメーカ端末２の処理について説明する。この処理は、例えば、図８に示される処理に続いて実行される。

【０１２９】

ステップＳ５１において、メーカ端末２のＣＰＵ３１は、記憶部３８に保存されている秘密鍵（Ｋｐｒｉ（メーカ））を用いて、ユーザ端末１から送信されてきた商品情報、ユーザ情報、および、メーカ名や連絡先などを表す情報を含むメーカ情報に対応する署名情報を生成する。例えば、ＣＰＵ３１は、商品情報、ユーザ情報、およびメーカ情報にハッシュ関数を適用し、得られたメッセージダイジェストを、秘密鍵（Ｋｐｒｉ（メーカ））を用いて暗号化し、署名情報を生成する。

【０１３０】

ＣＰＵ３１は、ステップＳ５２に進み、通信部３９を制御し、商品情報、ユーザ情報、メーカ情報、および、ステップＳ５１で生成した署名情報を含む配送依頼情報を配送業者端末３に送信する。

【０１３１】

次に、図１１のフローチャートを参照して、図１０の処理に対応して実行される、配送業者端末３の配送依頼確認処理について説明する。

【０１３２】

ステップＳ６１において、配送業者端末３のＣＰＵ５１は、メーカ端末２から配送依頼情報が送信されてきたか否かを判定し、送信されてきたと判定した場合、ステップＳ６２に進み、通信部５９を制御し、配送依頼情報を受信する。

【０１３３】

ステップＳ６３において、ＣＰＵ５１は、配送依頼情報に含まれるメーカ情報を認証局４に送信し、メーカ端末２により管理されている秘密鍵（Ｋｐｒｉ（メーカ））に対応する公開鍵（Ｋｐｕｂ（メーカ））の送信を要求する。

【０１３４】

認証局４においては、配送業者端末３からの要求に応じて公開鍵（Ｋｐｕｂ（メーカ））が読み出され、配送業者端末３に対して送信される。

【０１３５】

ステップＳ６４において、ＣＰＵ５１は、公開鍵（Ｋｐｕｂ（メーカ））を含む証明書が

認証局４から送信されてきたか否かを、通信部５９からの出力に基づいて判定し、証明書が送信されてきたと判定するまで待機する。

【０１３６】

ＣＰＵ５１は、ステップＳ６４において、証明書が送信されてきたと判定した場合、ステップＳ６５に進み、それを受信する。

【０１３７】

ステップＳ６６において、ＣＰＵ５１は、メーカ端末２から送信されてきた配送依頼情報の正当性を確認すべく、商品情報、ユーザ情報、およびメーカ情報にハッシュ関数を適用し、メッセージダイジェストを生成する。また、ＣＰＵ５１は、ステップＳ６７において、配送依頼情報に含まれる署名情報（メーカ端末２により管理されている秘密鍵（$K_{s_{メーカ}}$）により暗号化され、生成された署名情報）を、認証局４から送信されてきた公開鍵（$K_{p_{メーカ}}$）を用いて復号し、メッセージダイジェストを生成する。

【０１３８】

ＣＰＵ５１は、ステップＳ６８において、ステップＳ６６で生成したメッセージダイジェストと、ステップＳ６７で生成したメッセージダイジェストが一致するか否かを判定する。ＣＰＵ５１は、ステップＳ６８において、それらのメッセージダイジェストが一致しないと判定した場合、それは、メーカ端末２から送信されてきた配送依頼情報に対して改竄等が施されたおそれがあり、信頼できない情報であることを表しているため、ステップＳ６９に進み、配送の依頼を受けることができないことをメーカ端末２に対して通知する。

【０１３９】

一方、ステップＳ６８において、ＣＰＵ５１は、ステップＳ６６で生成したメッセージダイジェストと、ステップＳ６７で生成したメッセージダイジェストが一致すると判定した場合、ステップＳ７０に進み、登録されている配送人の中から、ユーザにより指定された配送先に商品を配送する配送人を選択する。

【０１４０】

ＣＰＵ５１は、ステップＳ７１において、ステップＳ７０で選択した配送人が有するＩＤカードに配設されているＰＫＩチップ５に、ユーザ情報、商品情報、およびメーカ情報を記憶させる。なお、ＰＫＩチップ５が、商品の表面に貼付される形で受取人に提供される場合、ユーザ情報、商品情報、およびメーカ情報が書き込まれたＰＫＩチップ５が商品（ユーザが注文した商品）の表面に貼付される。

【０１４１】

例えば、ＣＰＵ５１は、リーダライタ６０を制御して電磁波を輻射し、リーダライタ６０に近接されているＰＫＩチップ５（ＩＤカード）に誘起電力を発生させ、電磁波を介して、ユーザ情報、商品情報、およびメーカ情報をメモリ８４に記憶させる。

【０１４２】

以上のように、メーカ端末２から送信されてきた配送依頼情報の正当性が確認されたときにのみ、配送の依頼が受け付けられるため、仮に、配送依頼情報が改竄され、配送先の情報が書き換えられた場合であっても、書き換えられた配送先に商品が配送されるなどの事態を抑制することができる。すなわち、ＰＫＩのシステムにより、改竄等が施されることなく送信されてきた、信頼できるユーザ情報、商品情報、およびメーカ情報のみがＰＫＩチップ５に保存されることになる。

【０１４３】

次に、図１２のフローチャートを参照して、図１１の処理に対応して実行される、ＰＫＩチップ５の保存処理について説明する。

【０１４４】

ステップＳ８１において、ＰＫＩチップ５のＣＰＵ８１は、通信部８２からの出力に基づいて、ユーザ情報、商品情報、およびメーカ情報を保存することが指示されたか否かを判定し、それらの情報が、配送業者端末３のリーダライタ６０から輻射される電磁波を介して送信されてくるまで待機する。なお、リーダライタ６０から輻射される電磁波がループアンテナにおいて受信されたとき、誘起電力に基づいて電源供給部８５により生成された

直流電源が、ＰＫＩチップ５の各部に供給されている。

【０１４５】

ＣＰＵ８１は、ステップＳ８１において、配送業者端末３のリーダライタ６０から、ユーザ情報、商品情報、およびメーカ情報が送信され、それらの情報を保存することが指示されたと判定した場合、ステップＳ８２に進み、ユーザ情報、商品情報、およびメーカ情報（配送に関連する情報）をメモリ８４に記憶させる。

【０１４６】

次に、図１３のフローチャートを参照して、ユーザ端末１、メーカ端末２、および配送業者端末３からの要求に応じて、公開鍵を発行する認証局４の処理について説明する。

【０１４７】

認証局のＣＰＵ１０１は、ステップＳ９１において、公開鍵の発行が要求されたか否かを判定し、発行が要求されたと判定するまで待機する。

【０１４８】

ＣＰＵ１０１は、図８のステップＳ１３におけるメーカ端末２の処理により、図９のステップＳ３４におけるユーザ端末１の処理により、または、図１１のステップＳ６３における配送業者端末３の処理により、公開鍵の発行が要求されたと判定した場合、ステップＳ９２に進み、要求されている公開鍵を、記憶部１０８に構築されているデータベースから読み出す。読み出された公開鍵は、ステップＳ９３において発行される（送信される）。

【０１４９】

以上の処理により、ユーザ端末１からの要求に応じて、メーカの公開鍵（$K_{p_{メーカ}}$（メーカ））と配送業者の公開鍵（$K_{p_{配送業者}}$（配送業者））が発行され、メーカ端末２からの要求に応じて、ユーザの公開鍵（$K_{p_{ユーザ}}$（ユーザ））が発行される。また、配送業者端末３からの要求に応じて、メーカの公開鍵（$K_{p_{メーカ}}$（メーカ））が発行される。

【０１５０】

次に、図１４および図１５のフローチャートを参照して、商品とともに配送されてきたＰＫＩチップ５との間で署名情報の検証を行い、商品を確認するユーザ端末１の処理について説明する。

【０１５１】

この処理は、配送人が、ユーザにより指定された配送先に商品（注文された商品）を配送し、自分自身のＩＤカードをユーザに提示することに応じて、ユーザがユーザ端末１のリーダライタ２０を近接させることにより行われる。

【０１５２】

ステップＳ１０１において、ユーザ端末１のＣＰＵ１１は、リーダライタ２０を制御し、ＰＫＩチップ５（ＩＤカード）を検出するための電磁波を輻射する。ＣＰＵ１１は、ステップＳ１０２において、輻射された電磁波に対するＰＫＩチップ５からの応答に基づいて、ＰＫＩチップ５が検出されたか否かを判定し、ＰＫＩチップ５が検出されたと判定するまで待機する。

【０１５３】

ステップＳ１０２において、ＣＰＵ１１は、ＰＫＩチップ５が検出されたと判定した場合、ステップＳ１０３に進み、リーダライタ２０を制御し、商品の確認要求をＰＫＩチップ５に送信する。

【０１５４】

例えば、確認要求が受信されることに応じて、ＰＫＩチップ５は、メモリ８４に記憶されているユーザ情報、商品情報、メーカ情報、および、それらの情報に対応する、ＰＫＩチップ５に保存されている秘密鍵により生成された署名情報を送信してくるため（図１６のステップＳ１３４）、ＣＰＵ１１は、ステップＳ１０４において、ユーザ情報、商品情報、メーカ情報、および署名情報がＰＫＩチップ５から送信されてきたか否かを判定し、送信されてきたと判定するまで待機する。

【０１５５】

ステップＳ１０４において、ＣＰＵ１１は、ユーザ情報、商品情報、メーカ情報、および

、それらの情報に対応する署名情報が送信されてきたと判定した場合、ステップＳ１０５に進み、リーダライタ２０を制御し、それらの情報を受信する（読み出す）。

【０１５６】

ＣＰＵ１１は、ステップＳ１０６において、図９のステップＳ４０の処理により、記憶部１８に予め保存していた配送業者の公開鍵（K_{pub}（配送業者））を読み出し、ＰＫＩチップ５から送信されてきた署名情報の検証を行う。すなわち、ＣＰＵ１１は、ステップＳ１０７に進み、ＰＫＩチップ５から送信されてきたユーザ情報、商品情報、およびメーカ情報にハッシュ関数を適用し、メッセージダイジェストを生成する。

【０１５７】

また、ＣＰＵ１１は、ステップＳ１０８において、記憶部１８から読み出した公開鍵（K_{pub}（配送業者））を用いて、ＰＫＩチップ５から送信されてきた署名情報を復号し、メッセージダイジェストを生成する。

【０１５８】

ステップＳ１０９において、ＣＰＵ１１は、ステップＳ１０７で生成したメッセージダイジェストと、ステップＳ１０８で生成したメッセージダイジェストが一致するか否かを判定し、一致しないと判定した場合、ステップＳ１１０に進み、商品の確認ができなかったことを通知するメッセージを表示する。例えば、商品の受け取りを中止することを促すメッセージがユーザに提示される。

【０１５９】

一方、ステップＳ１０９において、ステップＳ１０７で生成したメッセージダイジェストと、ステップＳ１０８で生成したメッセージダイジェストが一致すると判定した場合、ＣＰＵ１１は、ステップＳ１１１に進み、無作為情報としての所定の桁数の乱数を生成する。生成した乱数は、ステップＳ１１２において、リーダライタ２０からＰＫＩチップ５に送信される。

【０１６０】

ＰＫＩチップ５においては、保存されている秘密鍵を用いて、ユーザ端末１から送信されてきた乱数に対応する署名情報が生成され、それがユーザ端末１に対して送信される（図１６のステップＳ１３８）。

【０１６１】

ステップＳ１１３において、ＣＰＵ１１は、リーダライタ２０からの出力に基づいて、ＰＫＩチップ５から署名情報が送信されてきたか否かを判定し、送信されてきたと判定するまで待機する。

【０１６２】

ＣＰＵ１１は、ステップＳ１１３において、乱数に対応する署名情報がＰＫＩチップ５から送信されてきたと判定した場合、ステップＳ１１４に進み、それを受信する。

【０１６３】

ＣＰＵ１１は、ステップＳ１１５において、送信されてきた署名情報（乱数に対応して生成された署名情報）の正当性を確認すべく、ステップＳ１１１で生成した乱数にハッシュ関数を適用し、メッセージダイジェストを生成するとともに、ステップＳ１１６に進み、公開鍵（K_{pub}（配送業者））を用いて、ＰＫＩチップ５から送信されてきた署名情報を復号し、メッセージダイジェストを生成する。

【０１６４】

ステップＳ１１７において、ＣＰＵ１１は、ステップＳ１１５で生成したメッセージダイジェストと、ステップＳ１１６で生成したメッセージダイジェストが一致するか否かを判定し、一致しないと判定した場合、ステップＳ１１０に進み、商品の確認ができなかったため、商品の受け取りを中止することを促すメッセージを表示する。

【０１６５】

一方、ステップＳ１１７において、ステップＳ１１５で生成したメッセージダイジェストと、ステップＳ１１６で生成したメッセージダイジェストが一致すると判定した場合、ＣＰＵ１１は、ステップＳ１１８に進み、商品の確認ができたこと、すなわち、配送されて

きた商品は、ユーザ自身が注文したものであり、配送元は、ユーザが商品を注文したメーカであることを表す情報を表示する。

【０１６６】

例えば、ＣＰＵ１１は、ＰＫＩチップ５から読み出した商品情報に基づいて、配送されてきた商品の名称などを表示し、メーカ情報に基づいて、商品の配送元であるメーカの名称などを表示する。また、ユーザ情報に基づいて、注文主としてのユーザ本人の氏名や住所などが表示される。

【０１６７】

このように、ＰＫＩチップ５から取得された情報に基づいて対応する情報が表示されるため、ユーザは、商品を開封することなく中身を確認し、配送されてきた商品を信頼して受け取ることができる。

【０１６８】

また、受け取りの際に生成された乱数を利用して検証が行われるため、ＰＫＩチップ５に予め保存されている情報のみに基づいて、商品の正当性を判断する場合に較べて、より確実な判断を行うことができる。

【０１６９】

次に、図１６のフローチャートを参照して、図１４および図１５の処理に対応して実行される、ＰＫＩチップ５の確認処理について説明する。

【０１７０】

ステップＳ１３１において、ＰＫＩチップ５のＣＰＵ８１は、商品の確認要求が送信されてきたか否かを通信部８２からの出力に基づいて判定し、送信されてきたと判定するまで待機する。ユーザ端末１においては、リーダライタ２０から電磁波が輻射され、その輻射範囲内においてＰＫＩチップ５が検出されたとき、ＰＫＩチップ５に対して商品の確認要求が送信される（図１４のステップＳ１０３）。

【０１７１】

ＣＰＵ８１は、ステップＳ１３１において、ユーザ端末１から確認要求が送信されてきたと判定した場合、ステップＳ１３２に進み、メモリ８４から秘密鍵（$K_{s,i}$（配送業者））を読み出す。

【０１７２】

ＣＰＵ８１は、ステップＳ１３３において、演算部８３を制御し、ステップＳ１３２で読み出した秘密鍵（$K_{s,i}$（配送業者））を用いて、メモリ８４に保存されているユーザ情報、商品情報、およびメーカ情報に対応する署名情報を生成し、生成した署名情報を、ステップＳ１３４において、ユーザ情報、商品情報、およびメーカ情報とともにユーザ端末１に対して送信する。

【０１７３】

送信された署名情報の検証が行われ、ＰＫＩチップ５により保存されている情報の正当性が確認されたとき、ユーザ端末１からは、所定の桁数の乱数が送信されてくる（図１５のステップＳ１１２）ため、ＣＰＵ８１は、ステップＳ１３５において、乱数が送信されてきたか否かを判定し、送信されてきたと判定するまで待機する。

【０１７４】

ＣＰＵ８１は、ステップＳ１３５において、乱数が送信されてきたと判定した場合、ステップＳ１３６に進み、それを受信する。

【０１７５】

ＣＰＵ８１は、ステップＳ１３７において、メモリ８４に記憶されている秘密鍵（$K_{s,i}$（配送業者））を用いて、乱数に対応する署名情報を生成し、ステップＳ１３８に進み、生成した署名情報をユーザ端末１に送信する。

【０１７６】

ユーザ端末１においては、ステップＳ１３８において送信された署名情報に基づいて署名情報の検証が行われ（図１５のステップＳ１１７）、署名情報が正当であることが検証されたとき、商品を安全に受け取ることができることを通知するメッセージが表示部に表示

される（図１５のステップＳ１１８）。

【０１７７】

以上のように、ＰＫＩのシステムにより信頼できる情報が記憶されたＰＫＩチップ５との間で、商品を受け取る直前に生成された乱数に対応する署名情報に基づいて、商品の正当性の検証が行われるため、ユーザは、配送されてきた商品が、本当に自分が注文した商品であるかを開封前に確実に確認することができる。また、その商品の検証は、配送人のＩＤカードや商品に貼付されているＰＫＩチップ５とリーダライタの間で非接触の近距離無線通信により行われるため、ユーザは、リーダライタを近接させるだけで、容易に、その検証を行うことができる。

【０１７８】

以上においては、メーカ端末２に対する商品の注文と、配送されてきた商品の検証が、１つのユーザ端末１により行われるとしたが、それらの処理がそれぞれ異なる端末により行われるようにしてもよい。この場合、ユーザは、商品を受け取るとき、ＰＫＩチップ５に記憶されている情報を検証するため公開鍵（ＰＫＩチップ５に保存されている秘密鍵に対応する公開鍵）が保存された端末（リーダライタ）のみを保持し、配送人に応対する。

【０１７９】

なお、ユーザ端末１とＰＫＩチップ５との間で行われる検証処理は、近距離で行われる無線通信であれば、例えば、ＩＥＥＥ（Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃｓ Ｅｎｇｉｎｅｅｒｓ）８０２．１１ａまたは８０２．１１ｂなどのいわゆる無線ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）やＢｌｕｅｔｏｏｔｈ、或いは、赤外線による近距離通信などの様々な通信方式により実行させることができる。

【０１８０】

以上においては、商品とともに配送されるＰＫＩチップ５には、ユーザ情報、商品情報、およびメーカ情報が記憶されるとしたが、それらの情報のうちの少なくともいずれか１つが記憶されるようにしてもよい。例えば、ユーザ情報のみがＰＫＩチップ５に記憶されている場合、ユーザは、署名情報の検証後にユーザ端末１の表示部に表示される情報を参照することで、配送されてきた商品が、本当に自分が注文した商品であるか否かを確認することができる。すなわち、改竄等が施されていないユーザ情報がＰＫＩチップ５に保存されている場合、ユーザ端末１の表示部には、注文主であるユーザ自身の氏名や住所などが表示されることになる。

【０１８１】

また、同様に、商品情報のみがＰＫＩチップ５に記憶されており、それが正当なものである場合、ユーザ端末１の表示部には、ユーザ自身が注文した商品の名称や個数が表示されるため、ユーザは、表示される情報を参照することで、開封前に、商品の中身を確認することができる。

【０１８２】

さらに、メーカ情報のみがＰＫＩチップ５に記憶されており、それが正当なものである場合、ユーザ端末１の表示部には、商品の注文先であるメーカの名称などが表示されるため、ユーザは、表示される情報を参照することで、商品の配送元を確認することができる。

【０１８３】

以上においては、メーカ端末２を管理するメーカ、配送業者端末３を管理する配送業者がそれぞれ異なるとしたが、メーカが配送業者を兼ねるなど、需用者側と供給者側において、それぞれ、システム構成の変更が可能である。

【０１８４】

メーカが配送業者を兼ねる場合、本発明を適用した配送システムは、例えば、図１７に示されるように構成される。

【０１８５】

ユーザ端末１は、ユーザからの指示に従って商品を注文するとき、メーカ端末２に対し、商品情報とユーザ情報、および、それらの情報に対応する署名情報（ユーザ端末１により

管理されている秘密鍵により暗号化され、生成された署名情報）を含む注文情報を送信する。注文情報を受信したメーカ端末２は、注文情報の正当性を確認すべく、認証局４に対して、ユーザ端末１において管理されている秘密鍵に対応する公開鍵の送信を要求し、要求に応じて送信されてきた公開鍵を用いて、注文情報に含まれる署名情報の検証を行う。

【０１８６】

メーカ端末２は、注文情報の正当性が確認できたとき、ユーザ端末１に対して注文受付情報を送信し、注文を受け付けたことを通知する。この注文受付情報には、例えば、図１の配送システムにおける配送業者情報に対応する、配送日時や配送人などを表す情報や、その情報に対応して、メーカ端末２により管理されている秘密鍵により暗号化され、生成された署名情報が含まれる。

【０１８７】

また、メーカ端末２は、ユーザ情報、商品情報、およびメーカ情報をＰＫＩチップ５に記憶させ、ＰＫＩチップ５を商品６とともにユーザ端末１に配送する。

【０１８８】

ユーザ端末１においては、注文受付情報がメーカ端末２から送信されてきたとき、メーカ端末２において管理されている秘密鍵に対応する公開鍵が認証局４から取得され、商品とともに配送されてきたＰＫＩチップ５との間で行われる検証処理において、その公開鍵が利用される。

【０１８９】

このように、構成を変更した場合であっても、ユーザは、配送される商品が正当なものであるか否かを、容易に、かつ確実に検証することができる。

【０１９０】

さらに、図１７の配送システムにおいて、メーカが、配送業者だけでなく認証局４の管理者をも兼ねるようにしてもよいし、注文が受け付けられたとき、メーカ端末２から認証局４に対し、メーカ端末２において管理されている秘密鍵に対応する公開鍵をユーザ端末１に送信することが要求されるようにしてもよい。この要求に応じて認証局４から送信された公開鍵を利用させることによっても、商品とともに配送されてくるＰＫＩチップ５との間で、署名情報の検証処理をユーザ端末１に実行させることができる。

【０１９１】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。

【０１９２】

一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば、汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【０１９３】

この記録媒体は、図２に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク２２（フレキシブルディスクを含む）、光ディスク２３（ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｋ－Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ），ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ）を含む）、光磁気ディスク２４（ＭＤ（登録商標）（Ｍｉｎｉ－Ｄｉｓｋ）を含む）、もしくは半導体メモリ２５などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているＲＯＭ１２や、記憶部１８に含まれるハードディスクなどで構成される。

【０１９４】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１９５】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表わすものである。

【０１９６】

【発明の効果】

本発明によれば、容易に、かつ確実に、配送されてきた商品の正当性を検証することができる。

【０１９７】

また、本発明によれば、送受信される情報を信頼できるものとすることができる。

【図面の簡単な説明】

【図１】本発明を適用した商品配送システムの構成例を示す図である。

【図２】図１のユーザ端末の構成例を示すブロック図である。

【図３】図１のメーカ端末の構成例を示すブロック図である。

【図４】図１の配送業者端末の構成例を示すブロック図である。

【図５】図１のＰＫＩチップの構成例を示すブロック図である。

【図６】図１の認証局の構成例を示すブロック図である。

【図７】ユーザ端末の注文処理について説明するフローチャートである。

【図８】図７の処理に対応して実行される、メーカ端末の受注処理について説明するフローチャートである。

【図９】ユーザ端末の検証処理について説明するフローチャートである。

【図１０】メーカ端末の配送依頼処理について説明するフローチャートである。

【図１１】図１０の処理に対応して実行される、配送業者端末の配送依頼確認処理について説明するフローチャートである。

【図１２】図１１の処理に対応して実行される、ＰＫＩチップの保存処理について説明するフローチャートである。

【図１３】認証局の公開鍵発行処理について説明するフローチャートである。

【図１４】ユーザ端末の商品確認処理について説明するフローチャートである。

【図１５】ユーザ端末の商品確認処理について説明する、図１４に続くフローチャートである。

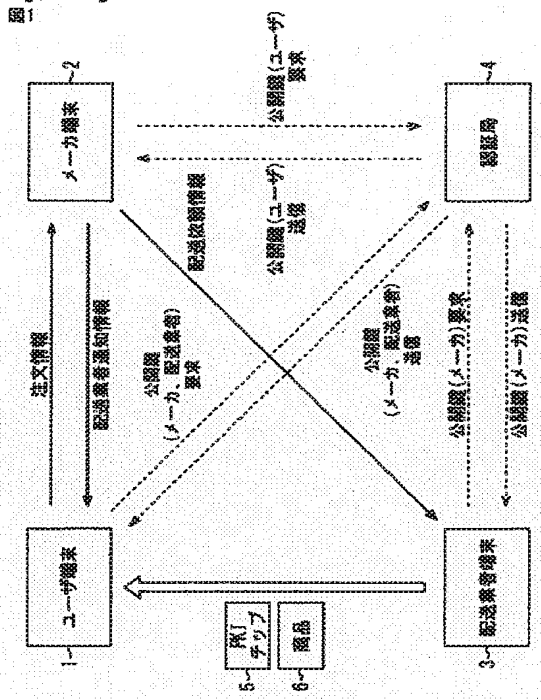
【図１６】図１４および図１５の処理に対応して実行される、ＰＫＩチップの確認処理について説明するフローチャートである。

【図１７】本発明を適用した配送システムの他の構成例を示す図である。

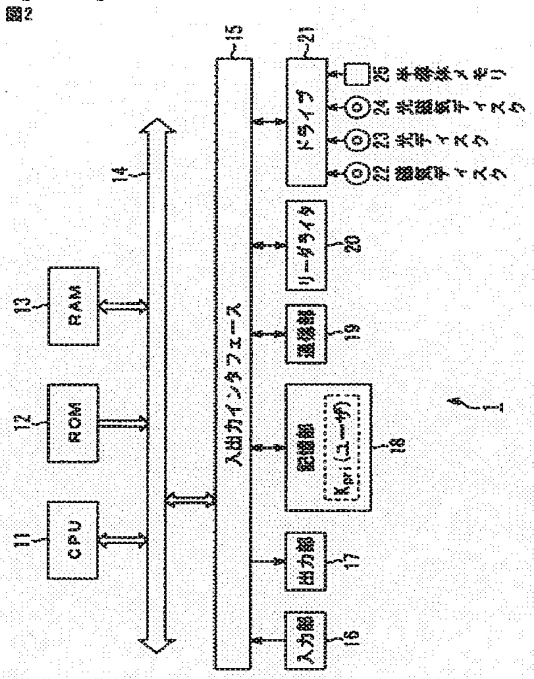
【符号の説明】

１　ユーザ端末１，　２　メーカ端末，　３　配送業者端末，　４　認証局，５　ＰＫＩチップ，　６　商品

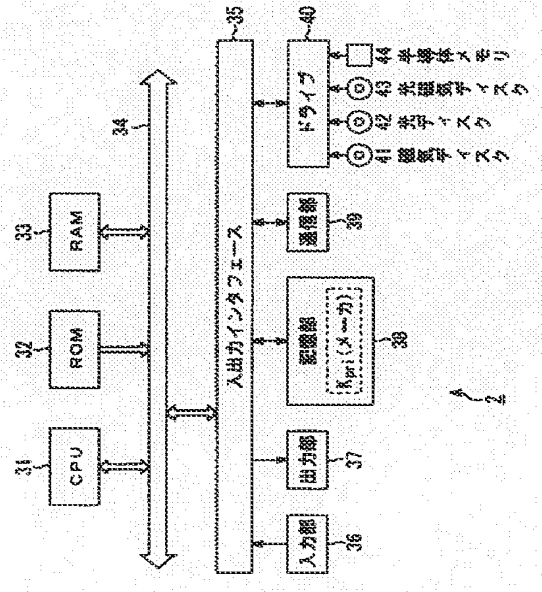
【図１】


メーカ端末
2
公開鍵(ユーザ)要求
認証局
4
注文情報
配送業者通知情報
公開鍵(メーカ,配送業者)要求
配送依頼情報
公開鍵(ユーザ)送信
公開鍵(メーカ,配送業者)送信
公開鍵(メーカ)要求
公開鍵(メーカ)送信
ユーザ端末
1
配送業者端末
3
ICチップ
5
商品
6

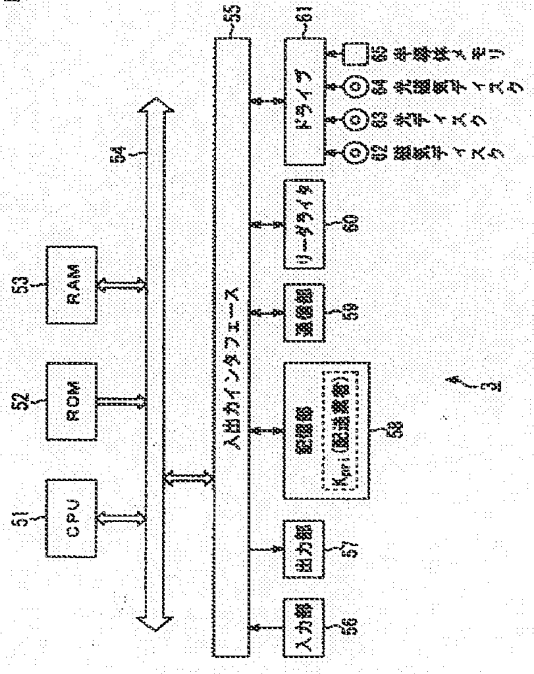
【図２】


RAM
13
ROM
12
CPU
11
入出力インタフェース
15
14
ドライブ
21
光磁気ディスク
22
光ディスク
23
半導体メモリ
25
リーダライタ
20
通信部
19
記憶部
18
入力部
16
出力部
17
1

【図３】

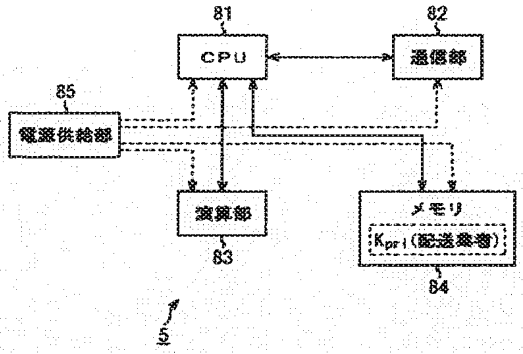

RAM
33
ROM
32
CPU
31
入出力インタフェース
35
34
ドライブ
40
光磁気ディスク
41
光ディスク
42
半導体メモリ
44
通信部
39
記憶部
38
入力部
36
出力部
37
2

【図４】


RAM
53
ROM
52
CPU
51
入出力インタフェース
55
54
ドライブ
61
光磁気ディスク
62
光ディスク
63
半導体メモリ
65
リーダライタ
60
通信部
59
記憶部
58
入力部
56
出力部
57
3

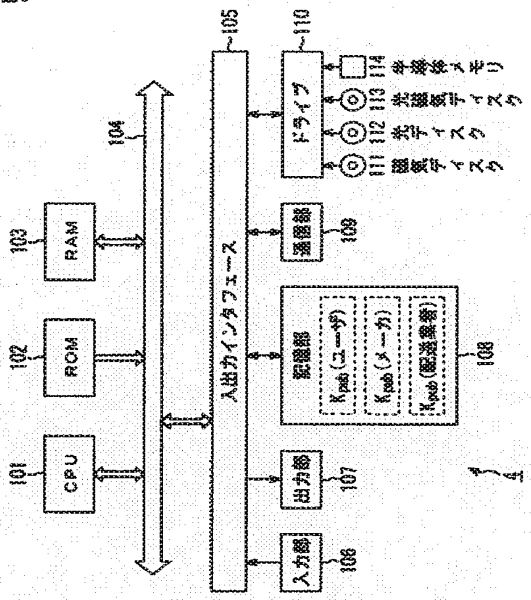
【図５】

図5



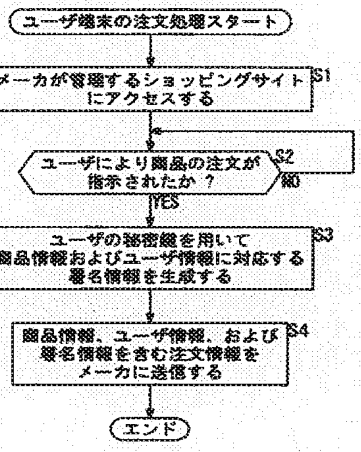
【図６】

図6



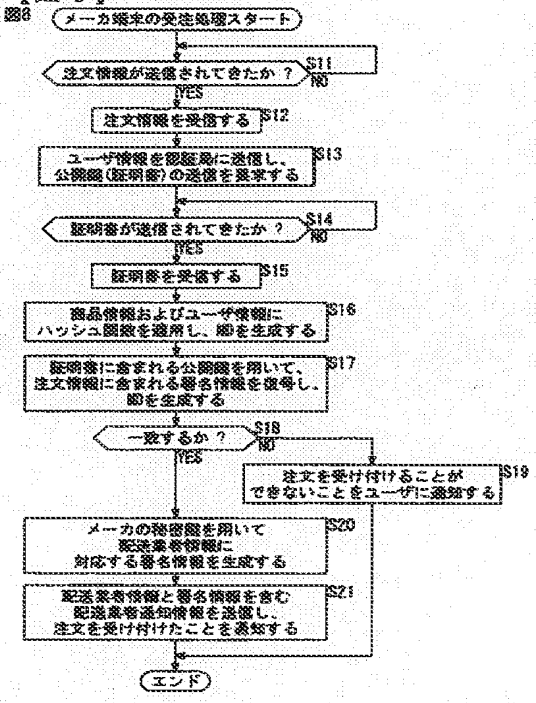
【図７】

図7



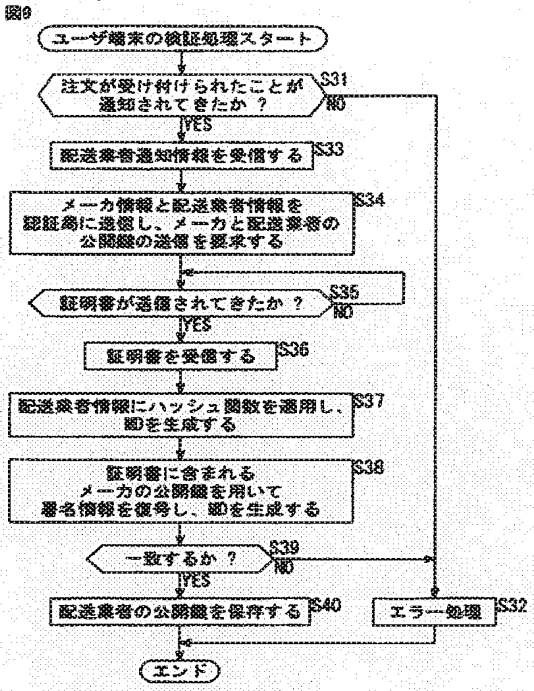
【図８】

図8



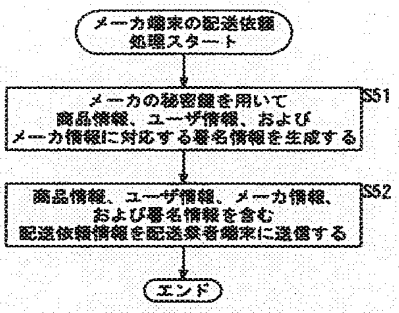
【図９】

図9



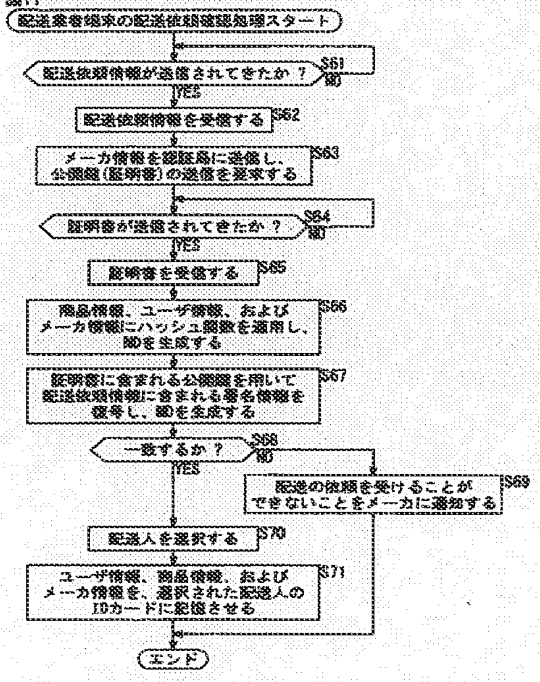
【図１０】

図10



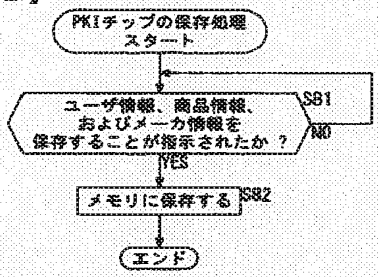
【図１１】

図11



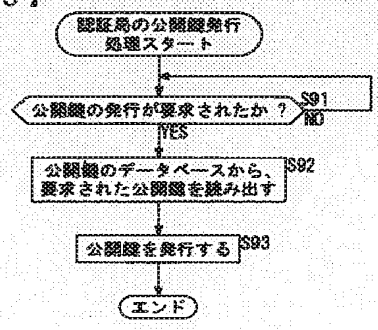
【図１２】

図12



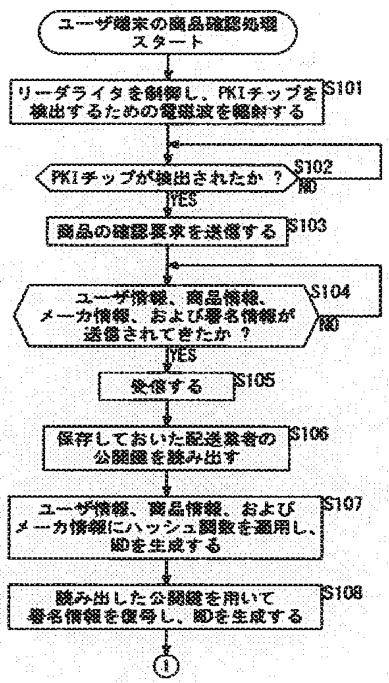
【図１３】

図13



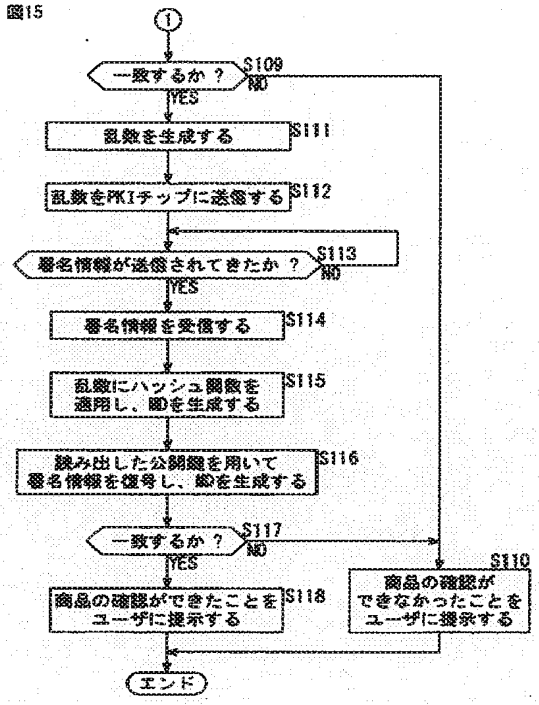
【図１４】

図14



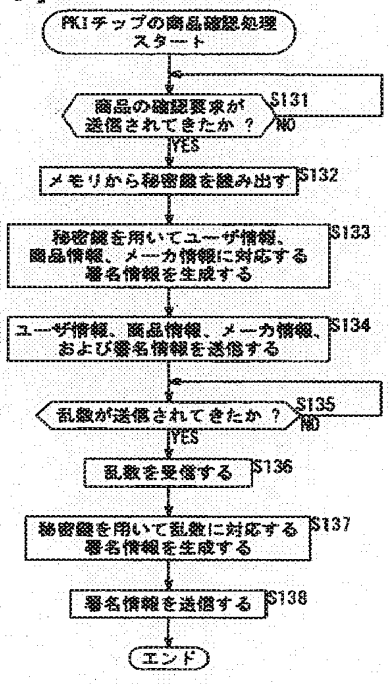
【図１５】

図15



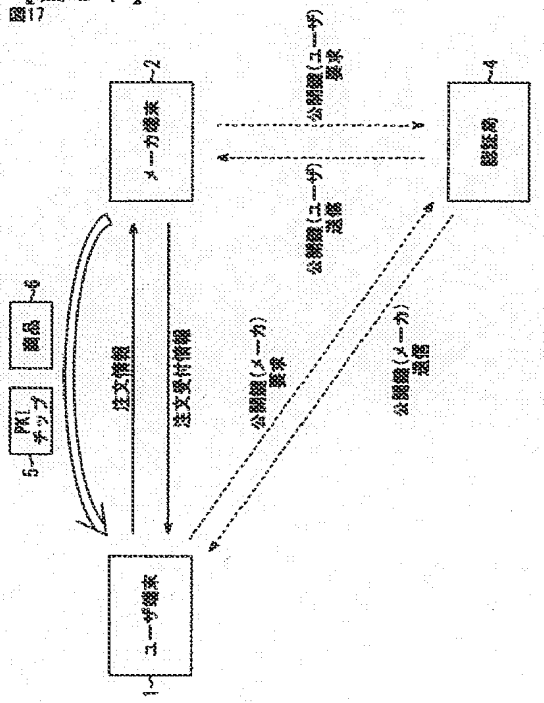
【図１６】

図16



【図１７】

図17



フロントページの続き

(51)Int.Cl.'	F I			テーマコード（参考）
	G06F	17/60	334	
	G06F	17/60	512	
	G06K	17/00	F	
	G06K	17/00	T	

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成17年10月27日(2005.10.27)

【公開番号】特開2004-88534(P2004-88534A)
【公開日】平成16年3月18日(2004.3.18)
【年通号数】公開・登録公報2004-011
【出願番号】特願2002-248108(P2002-248108)
【国際特許分類第７版】
Ｈ０４Ｌ　9/32
Ｂ６５Ｇ　61/00
Ｇ０６Ｆ　17/60
Ｇ０６Ｋ　17/00
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｂ６５Ｇ　61/00　２１０
Ｂ６５Ｇ　61/00　５２２
Ｇ０６Ｆ　17/60　１１４
Ｇ０６Ｆ　17/60　３０２Ａ
Ｇ０６Ｆ　17/60　３３４
Ｇ０６Ｆ　17/60　５１２
Ｇ０６Ｋ　17/00　Ｆ
Ｇ０６Ｋ　17/00　Ｔ

【手続補正書】
【提出日】平成17年8月29日(2005.8.29)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正の内容】
【発明の名称】検証システムおよび方法、情報処理装置および方法、受注管理装置および方法、配送管理装置および方法
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】　配送されてきた商品に関連する情報を検証する情報処理装置と、前記商品とともに配送される情報管理チップからなる検証システムにおいて、
前記情報処理装置は、
前記情報管理チップにより保存されている秘密鍵に対応する公開鍵を取得する取得手段と、
無作為情報を生成する無作為情報生成手段と、
前記無作為情報生成手段により生成された前記無作為情報を、近距離無線通信を介して前記情報管理チップに送信する無作為情報送信手段と、
前記無作為情報送信手段により送信された前記無作為情報に対応するものとして前記情報管理チップにより生成された署名情報を、前記近距離無線通信を介して受信する署名情報受信手段と、

前記署名情報受信手段により受信された前記署名情報を、前記取得手段により取得された前記公開鍵を用いて検証する検証手段と
を備え、
前記情報管理チップは、
前記秘密鍵を記憶する記憶手段と、
前記商品の受取人により操作される前記情報処理装置から、前記近距離無線通信を介して送信された前記無作為情報を受信する無作為情報受信手段と、
前記記憶手段により記憶されている前記秘密鍵を用いて、前記無作為情報受信手段により受信された前記無作為情報に対応する前記署名情報を生成する署名情報生成手段と、
前記署名情報生成手段により生成された前記署名情報を、前記近距離無線通信を介して前記情報処理装置に送信する署名情報送信手段と
を備えることを特徴とする検証システム。
【請求項２】　配送されてきた商品に関連する情報を検証する情報処理装置と、前記商品とともに配送される情報管理チップからなる検証システムの検証方法において、
前記情報処理装置の情報処理方法は、
前記情報管理チップにより保存されている秘密鍵に対応する公開鍵を取得する取得ステップと、
無作為情報を生成する無作為情報生成ステップと、
前記無作為情報生成ステップの処理により生成された前記無作為情報を、近距離無線通信を介して前記情報管理チップに送信する無作為情報送信ステップと、
前記無作為情報送信ステップの処理により送信された前記無作為情報に対応するものとして前記情報管理チップにより生成された署名情報を、前記近距離無線通信を介して受信する署名情報受信ステップと、
前記署名情報受信ステップの処理により受信された前記署名情報を、前記取得ステップの処理により取得された前記公開鍵を用いて検証する検証ステップと
を含み、
前記情報管理チップの情報管理方法は、
前記秘密鍵を記憶する記憶ステップと、
前記商品の受取人により操作される前記情報処理装置から、前記近距離無線通信を介して送信された前記無作為情報を受信する無作為情報受信ステップと、
内部に記憶されている前記秘密鍵を用いて、前記無作為情報受信ステップの処理により受信された前記無作為情報に対応する前記署名情報を生成する署名情報生成ステップと、
前記署名情報生成ステップの処理により生成された前記署名情報を、前記近距離無線通信を介して前記情報処理装置に送信する署名情報送信ステップと
を含むことを特徴とする検証方法。
【請求項３】　配送されてきた商品に関連する情報を検証する情報処理装置において、
前記商品とともに配送されてきた情報管理チップにより管理されている第１の秘密鍵に対応する公開鍵を取得する取得手段と、
無作為情報を生成する無作為情報生成手段と、
前記無作為情報生成手段により生成された前記無作為情報を、近距離無線通信を介して前記情報管理チップに送信する送信手段と、
前記送信手段により送信された前記無作為情報に対応するものとして前記情報管理チップにより生成された第１の署名情報を、前記近距離無線通信を介して受信する署名情報受信手段と、
前記署名情報受信手段により受信された前記第１の署名情報を、前記取得手段により取得された前記公開鍵を用いて検証する第１の検証手段と
を備えることを特徴とする情報処理装置。
【請求項４】　前記第１の秘密鍵を用いて前記情報管理チップにより生成された、前

記商品の配送に関する配送関連情報に対応する第２の署名情報を、前記配送関連情報とともに前記近距離無線通信を介して受信する配送関連情報受信手段と、
前記配送関連情報受信手段により受信された前記第２の署名情報を、前記公開鍵を用いて検証する第２の検証手段と
をさらに備え、
前記送信手段は、前記第２の検証手段により前記第２の署名情報の正当性が確認されたとき、前記無作為情報を前記情報管理チップに送信する
ことを特徴とする請求項３に記載の情報処理装置。
【請求項５】 前記第１の検証手段による検証結果を出力する検証結果出力手段をさらに備える
ことを特徴とする請求項３に記載の情報処理装置。
【請求項６】 第２の秘密鍵を記憶する記憶手段と、
前記記憶手段により記憶されている前記第２の秘密鍵を用いて、前記商品の識別情報を含む商品情報、および、前記商品の注文主に関するユーザ情報に対応する第２の署名情報を生成する署名情報生成手段と、
前記商品情報、前記ユーザ情報、前記署名情報生成手段により生成された前記第２の署名情報を含む注文情報を、前記商品の受注を管理する受注管理装置に対して送信し、前記商品を注文する注文手段と
をさらに備えることを特徴とする請求項３に記載の情報処理装置。
【請求項７】 配送されてきた商品に関連する情報を検証する情報処理装置の情報処理方法において、
前記商品とともに配送されてきた情報管理チップにより管理されている秘密鍵に対応する公開鍵を取得する取得ステップと、
無作為情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記無作為情報を、近距離無線通信を介して前記情報管理チップに送信する送信ステップと、
前記送信ステップの処理により送信された前記無作為情報に対応するものとして前記情報管理チップにより生成された署名情報を、前記近距離無線通信を介して受信する受信ステップと、
前記受信ステップの処理により受信された前記署名情報を、前記取得ステップの処理により取得された前記公開鍵を用いて検証する検証ステップと
を含むことを特徴とする情報処理方法。
【請求項８】 情報処理装置からの注文に応じて、商品の受注を管理する受注管理装置において、
前記商品の識別情報を含む商品情報、および、前記商品の注文主に関するユーザ情報、並びに、前記情報処理装置により保存されている第１の秘密鍵を用いて生成された、前記商品情報と前記ユーザ情報に対応する第１の署名情報を含む注文情報を、前記情報処理装置から受信する受信手段と、
前記ユーザ情報を認証局に送信し、前記第１の秘密鍵に対応する公開鍵の送信を要求する要求手段と、
前記要求手段による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記第１の署名情報の正当性を検証する検証手段と、
前記検証手段により前記第１の署名情報の正当性が確認されたとき、注文が成立したことを前記情報処理装置に通知する通知手段と
を備えることを特徴とする受注管理装置。
【請求項９】 情報処理装置からの注文に応じて、商品の受注を管理する受注管理装置の受注管理方法において、
前記商品の識別情報を含む商品情報、および、前記商品の注文主に関するユーザ情報、並びに、前記情報処理装置により保存されている秘密鍵を用いて生成された、前記商品情報と前記ユーザ情報に対応する署名情報を含む注文情報を、前記情報処理装置から受信す

る受信ステップと、
前記ユーザ情報を認証局に送信し、前記秘密鍵に対応する公開鍵の送信を要求する要求ステップと、
前記要求ステップの処理による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記署名情報の正当性を検証する検証ステップと、
前記検証ステップの処理により前記署名情報の正当性が確認されたとき、注文が成立したことを前記情報処理装置に通知する通知ステップと
を含むことを特徴とする受注管理方法。
【請求項１０】 商品の受注を管理する受注管理装置からの依頼に応じて、商品の配送を管理する配送管理装置において、
前記商品の識別情報を含む商品情報、前記商品の注文主に関するユーザ情報、前記受注管理装置の管理者に関する受注者情報、前記受注管理装置により管理される秘密鍵を用いて生成された、前記商品情報、前記ユーザ情報、および前記受注者情報に対応する署名情報を含む前記配送依頼情報を、前記受注管理装置から受信する受信手段と、
前記受注者情報を認証局に送信し、前記秘密鍵に対応する公開鍵の送信を要求する要求手段と、
前記要求手段による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記署名情報の正当性を検証する検証手段と、
前記検証手段により前記署名情報の正当性が確認されたとき、前記商品とともに配送される情報管理チップに、前記商品の配送に関する配送関連情報を記憶させる記憶制御手段と
を備えることを特徴とする配送管理装置。
【請求項１１】 商品の受注を管理する受注管理装置からの依頼に応じて、商品の配送を管理する配送管理装置の配送管理方法において、
前記商品の識別情報を含む商品情報、前記商品の注文主に関するユーザ情報、前記受注管理装置の管理者に関する受注者情報、前記受注管理装置により管理される秘密鍵を用いて生成された、前記商品情報、前記ユーザ情報、および前記受注者情報に対応する署名情報を含む前記配送依頼情報を、前記受注管理装置から受信する受信ステップと、
前記受注者情報を認証局に送信し、前記秘密鍵に対応する公開鍵の送信を要求する要求ステップと、
前記要求ステップの処理による要求に応じて前記認証局から送信されてきた前記公開鍵を用いて、前記署名情報の正当性を検証する検証ステップと、
前記検証ステップの処理により前記署名情報の正当性が確認されたとき、前記商品とともに配送される情報管理チップに、前記商品の配送に関する配送関連情報を記憶させる記憶制御ステップと
を含むことを特徴とする配送管理方法。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００１
【補正方法】変更
【補正の内容】
【０００１】
【発明の属する技術分野】
本発明は、検証システムおよび方法、情報処理装置および方法、受注管理装置および方法、配送管理装置および方法に関し、特に、配送されてきた荷物の中身や配送元、或いは、配送業者などの荷物の配送に関する様々な情報の正当性を、容易に、かつ確実に確認できるようにする検証システムおよび方法、情報処理装置および方法、受注管理装置および方法、配送管理装置および方法に関する。
【手続補正４】
【補正対象書類名】明細書

【補正対象項目名】００１６
【補正方法】削除
【補正の内容】
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】削除
【補正の内容】
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】削除
【補正の内容】
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】削除
【補正の内容】
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】削除
【補正の内容】
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】削除
【補正の内容】
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】削除
【補正の内容】
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】削除
【補正の内容】
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００３０
【補正方法】削除
【補正の内容】
【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００３１
【補正方法】削除
【補正の内容】
【手続補正１４】
【補正対象書類名】明細書

【補正対象項目名】００３３
【補正方法】削除
【補正の内容】
【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】００３４
【補正方法】削除
【補正の内容】
【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】００３５
【補正方法】削除
【補正の内容】
【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】００３６
【補正方法】削除
【補正の内容】
【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】００３７
【補正方法】削除
【補正の内容】
【手続補正１９】
【補正対象書類名】明細書
【補正対象項目名】００３８
【補正方法】削除
【補正の内容】
【手続補正２０】
【補正対象書類名】明細書
【補正対象項目名】００３９
【補正方法】削除
【補正の内容】
【手続補正２１】
【補正対象書類名】明細書
【補正対象項目名】００４０
【補正方法】削除
【補正の内容】
【手続補正２２】
【補正対象書類名】明細書
【補正対象項目名】００４３
【補正方法】変更
【補正の内容】
【００４３】
本発明の情報処理装置および方法においては、商品とともに配送されてきた情報管理チップにより保存されている秘密鍵に対応する公開鍵が取得され、無作為情報が生成される。また、生成された無作為情報が、近距離無線通信を介して情報管理チップに送信され、情報管理チップにより無作為情報に対応するものとして生成された署名情報が、近距離無線通信を介して受信され、公開鍵を用いて検証される。
【手続補正２３】

【補正対象書類名】明細書
【補正対象項目名】００４４
【補正方法】変更
【補正の内容】
【００４４】
本発明の受注管理装置および方法においては、商品の識別情報を含む商品情報、および、商品の注文主に関するユーザ情報、並びに、情報処理装置により保存されている第１の秘密鍵を用いて生成された、商品情報とユーザ情報に対応する第１の署名情報を含む注文情報が受信され、ユーザ情報が認証局に送信され、第１の秘密鍵に対応する公開鍵の送信が要求される。また、要求に応じて認証局から送信されてきた公開鍵を用いて、第１の署名情報の正当性が検証され、第１の署名情報の正当性が確認されたとき、注文が成立したことが情報処理装置に通知される。
【手続補正２４】
【補正対象書類名】明細書
【補正対象項目名】００４５
【補正方法】変更
【補正の内容】
【００４５】
本発明の配送管理装置および方法においては、商品の識別情報を含む商品情報、商品の注文主に関するユーザ情報、受注管理装置の管理者に関する受注者情報、受注管理装置により保存される秘密鍵を用いて生成された、商品情報、ユーザ情報、および受注者情報に対応する署名情報を含む配送依頼情報が受信され、受注者情報を認証局に送信が、秘密鍵に対応する公開鍵の送信が要求される。また、要求に応じて認証局から送信されてきた公開鍵を用いて、署名情報の正当性が検証され、署名情報の正当性が確認されたとき、商品とともに配送される情報管理チップに、商品の配送に関する配送関連情報が記憶される。
【手続補正２５】
【補正対象書類名】明細書
【補正対象項目名】００４６
【補正方法】削除
【補正の内容】

CLAIMS

[Claim(s)]
[Claim 1]
In an information processor which verifies information relevant to delivered goods, and a verification system which consists of an information management chip delivered with said goods,
Said information processor,
An acquisition means which acquires a public key corresponding to a secret key saved by said information management chip,
A random information creating means which generates random information,
A random information transmission means which transmits said random information generated by said random information creating means to said information management chip via short-distance-radio communication,
A signature information reception means which receives signature information generated by said information management chip as a thing corresponding to said random information transmitted by said random information transmission means via said short-distance-radio communication,
A verifying means which verifies said signature information received by said signature information reception means using said public key acquired by said acquisition means
A preparation,
Said information management chip,
A memory measure which memorizes said secret key,
A random information receiving means which receives said random information transmitted via said short-distance-radio communication from said information

processor operated by recipient of said goods,
A signature information creating means which generates said signature information corresponding to said random information received by said random information receiving means using said secret key memorized by said memory measure,
A signature information transmitting means which transmits said signature information generated by said signature information creating means to said information processor via said short-distance-radio communication
A verification system characterized by preparation ******.
[Claim 2]
In a verification method of an information processor which verifies information relevant to delivered goods, and a verification system which consists of an information management chip delivered with said goods,
An information processing method of said information processor,
An acquisition step which acquires a public key corresponding to a secret key saved by said information management chip,
A random information generation step which generates random information,
A random transmitting information step which transmits said random information generated by processing of said random information generation step to said information management chip via short-distance-radio communication,
A signature information receiving step which receives signature information generated by said information management chip as a thing corresponding to said random information transmitted by processing of said random transmitting information step via said short-distance-radio communication,
Verification steps which verify said signature information received by processing of said signature information receiving step using said public key acquired by processing of said acquisition step
An implication,
An information management method of said information management chip,
A memory step which memorizes said secret key,
A random information reception step which receives said random information transmitted via said short-distance-radio communication from said information processor operated by recipient of said goods,
A signature information generation step which generates said signature information corresponding to said random information received by processing of said random information reception step using said secret key memorized inside,
A signature information transmission step which transmits said signature information

generated by processing of said signature information generation step to said information processor via said short-distance-radio communication
****** -- a verification method characterized by things.
[Claim 3]
In an information processor which verifies information relevant to delivered goods,
An acquisition means which acquires a public key corresponding to the 1st secret key managed by the information management chip delivered with said goods,
A random information creating means which generates random information,
A transmitting means which transmits said random information generated by said random information creating means to said information management chip via short-distance-radio communication,
A signature information reception means which receives the 1st signature information generated by said information management chip as a thing corresponding to said random information transmitted by said transmitting means via said short-distance-radio communication,
The 1st verifying means that verifies said 1st signature information received by said signature information reception means using said public key acquired by said acquisition means
An information processor characterized by preparation ******.
[Claim 4]
A delivery pertinent information reception means which receives the 2nd signature information corresponding to delivery pertinent information about delivery of said goods generated by said information management chip using said 1st secret key via said short-distance-radio communication with said delivery pertinent information,
The 2nd verifying means that verifies said 2nd signature information received by said delivery pertinent information reception means using said public key
It prepares for a pan,
Said transmitting means transmits said random information to said information management chip, when the justification of said 2nd signature information is checked by said 2nd verifying means.
The information processor according to claim 3 characterized by things.
[Claim 5]
When the justification of said 1st signature information is checked by said 1st verifying means, it has further a delivery pertinent information output means which outputs said delivery pertinent information.
The information processor according to claim 4 characterized by things.

[Claim 6]
It has further a verification result output means which outputs a verification result by said 1st verifying means.
The information processor according to claim 3 characterized by things.
[Claim 7]
A memory measure which memorizes the 2nd secret key,
A signature information creating means which generates the 2nd signature information corresponding to merchandise information containing identification information of said goods, and User Information about the order Lord of said goods using said 2nd secret key memorized by said memory measure,
An order means to transmit ordering information including said merchandise information, said User Information, and said 2nd signature information generated by said signature information creating means to an order control device which manages an order received of said goods, and to order said goods
The information processor according to claim 3 preparing for a pan.
[Claim 8]
When it has been reported from said order control device that an order of said goods was accepted, it has further a request means which requires transmission of said public key corresponding to said 1st secret key from a certificate authority,
Said acquisition means acquires said public key transmitted from said certificate authority according to a demand by said request means.
The information processor according to claim 7 characterized by things.
[Claim 9]
In an information processing method of an information processor which verifies information relevant to delivered goods,
An acquisition step which acquires a public key corresponding to a secret key managed by the information management chip delivered with said goods,
A generation step which generates random information,
A transmission step which transmits said random information generated by processing of said generation step to said information management chip via short-distance-radio communication,
A receiving step which receives signature information generated by said information management chip as a thing corresponding to said random information transmitted by processing of said transmission step via said short-distance-radio communication,
Verification steps which verify said signature information received by processing of said receiving step using said public key acquired by processing of said acquisition

step
****** -- an information processing method characterized by things.
[Claim 10]
In a recording medium of a program which a computer which controls an information processor which verifies information relevant to delivered goods is made to execute,
An acquisition control step which controls acquisition of a public key corresponding to a secret key managed by the information management chip delivered with said goods,
A generation step which generates random information,
A transmission-control step which controls transmission to said information management chip performed via short-distance-radio communication of said random information generated by processing of said generation step,
A reception-control step which controls reception performed via said short-distance-radio communication of signature information generated by said information management chip as a thing corresponding to said random information transmitted by processing of said transmission-control step,
Verification steps which verify said signature information received by processing of said reception-control step using said public key acquired by processing of said acquisition step
****** -- a recording medium with which a program which a computer characterized by things can read is recorded.
[Claim 11]
To a computer which controls an information processor which verifies information relevant to delivered goods
An acquisition control step which controls acquisition of a public key corresponding to a secret key managed by the information management chip delivered with said goods,
A generation step which generates random information,
A transmission-control step which controls transmission to said information management chip performed via short-distance-radio communication of said random information generated by processing of said generation step,
A reception-control step which controls reception performed via said short-distance-radio communication of signature information generated by said information management chip as a thing corresponding to said random information transmitted by processing of said transmission-control step,
Verification steps which verify said signature information received by processing of said reception-control step using said public key acquired by processing of said acquisition step

A program making it perform.

[Claim 12]

In an order control device which manages an order received of goods according to an order from an information processor,

Merchandise information containing identification information of said goods, and User Information about the order Lord of said goods, And a reception means which receives ordering information including the 1st signature information corresponding to said merchandise information and said User Information generated using the 1st secret key saved by said information processor from said information processor,

A request means which transmits said User Information to a certificate authority, and requires transmission of a public key corresponding to said 1st secret key,

A verifying means which verifies the justification of said 1st signature information using said public key transmitted from said certificate authority according to a demand by said request means,

A reporting means which notifies said information processor that an order was materialized when the justification of said 1st signature information is checked by said verifying means

An order control device characterized by preparation ******.

[Claim 13]

A memory measure which memorizes the 2nd secret key,

A creating means which generates the 2nd signature information corresponding to said merchandise information, said User Information, and successful-bidder information about an administrator of said order control device using said 2nd secret key memorized by said memory measure,

A delivery request means to transmit delivery request information including said merchandise information, said User Information, said successful-bidder information, and said 2nd signature information generated by said creating means to a distribution control device which manages delivery of said goods, and to request delivery of said goods

The order control device according to claim 12 preparing for a pan.

[Claim 14]

In an order-receiving-control method of an order control device of managing an order received of goods according to an order from an information processor,

Merchandise information containing identification information of said goods, and User Information about the order Lord of said goods, And a receiving step which was generated using a secret key saved by said information processor and which receives

said merchandise information and ordering information including signature information corresponding to said User Information from said information processor,
A request step which transmits said User Information to a certificate authority, and requires transmission of a public key corresponding to said secret key,
Verification steps which verify the justification of said signature information using said public key transmitted from said certificate authority according to a demand by processing of said request step,
A notification step which notifies said information processor that an order was materialized when the justification of said signature information is checked by processing of said verification steps
****** -- an order-receiving-control method characterized by things.
[Claim 15]
In a recording medium of a program which a computer which controls an order control device which manages an order received of goods according to an order from an information processor is made to execute,
A reception-control step which was generated using merchandise information containing identification information of said goods, User Information about the order Lord of said goods, and a secret key saved by said information processor and which controls reception of said merchandise information and ordering information including signature information corresponding to said User Information,
A request step which controls transmission to a certificate authority of said User Information, and requires transmission of a public key corresponding to said secret key,
Verification steps which verify the justification of said signature information using said public key transmitted from said certificate authority according to a demand by processing of said request step,
A recording medium with which a program which a computer by which a notification control step which controls a notice to said information processor of an order having been materialized being included when the justification of said signature information is checked by processing of said verification steps can read is recorded.
[Claim 16]
To a computer which controls an order control device which manages an order received of goods according to an order from an information processor
A reception-control step which was generated using merchandise information containing identification information of said goods, User Information about the order Lord of said goods, and a secret key saved by said information processor and which

controls reception of said merchandise information and ordering information including signature information corresponding to said User Information,
A request step which controls transmission to a certificate authority of said User Information, and requires transmission of a public key corresponding to said secret key,
Verification steps which verify the justification of said signature information using said public key transmitted from said certificate authority according to a demand by processing of said request step,
A program performing a notification control step which controls a notice to said information processor of an order having been materialized when the justification of said signature information is checked by processing of said verification steps.
[Claim 17]
In a distribution control device which manages delivery of goods according to a request from an order control device which manages an order received of goods, Merchandise information containing identification information of said goods, User Information about the order Lord of said goods, A reception means which receives said delivery request information including said merchandise information, said User Information, and signature information corresponding to said successful-bidder information which were generated using a secret key managed by successful-bidder information about an administrator of said order control device, and said order control device from said order control device,
A request means which transmits said successful-bidder information to a certificate authority, and requires transmission of a public key corresponding to said secret key,
A verifying means which verifies the justification of said signature information using said public key transmitted from said certificate authority according to a demand by said request means,
A storage control means which makes an information management chip delivered with said goods memorize delivery pertinent information about delivery of said goods when the justification of said signature information is checked by said verifying means
A distribution control device characterized by preparation ******.
[Claim 18]
It has further a delivering means which delivers said information management chip with said goods.
The distribution control device according to claim 17 characterized by things.
[Claim 19]
At least one information on said merchandise information, said User Information, said

successful-bidder information, and delivery administrator information about a delivery administrator who manages delivery of said goods is included in said delivery pertinent information.
The distribution control device according to claim 17 characterized by things.
[Claim 20]
Said information management chip is delivered with said goods, when held by distribution company who is stuck on the surface of said goods or delivers said goods.
The distribution control device according to claim 17 characterized by things.
[Claim 21]
In a delivery management method of a distribution control device which manages delivery of goods according to a request from an order control device which manages an order received of goods,
Merchandise information containing identification information of said goods, User Information about the order Lord of said goods, A receiving step which receives said delivery request information including said merchandise information, said User Information, and signature information corresponding to said successful-bidder information which were generated using a secret key managed by successful-bidder information about an administrator of said order control device, and said order control device from said order control device,
A request step which transmits said successful-bidder information to a certificate authority, and requires transmission of a public key corresponding to said secret key,
Verification steps which verify the justification of said signature information using said public key transmitted from said certificate authority according to a demand by processing of said request step,
A storage control step which makes an information management chip delivered with said goods memorize delivery pertinent information about delivery of said goods when the justification of said signature information is checked by processing of said verification steps
****** -- a delivery management method characterized by things.
[Claim 22]
In a recording medium of a program which a computer which controls a distribution control device which manages delivery of goods according to a request from an order control device which manages an order received of goods is made to execute,
Merchandise information containing identification information of said goods, User Information about the order Lord of said goods, A reception-control step which controls reception of said delivery request information including said merchandise

information, said User Information, and signature information corresponding to said successful-bidder information which were generated using a secret key managed by successful-bidder information about an administrator of said order control device, and said order control device,
A request step which controls transmission to a certificate authority of said successful-bidder information, and requires transmission of a public key corresponding to said secret key,
Verification steps which verify the justification of said signature information using said public key transmitted from said certificate authority according to a demand by processing of said request step,
A storage control step which makes an information management chip delivered with said goods memorize delivery pertinent information about delivery of said goods when the justification of said signature information is checked by processing of said verification steps
****** -- a recording medium with which a program which a computer characterized by things can read is recorded.
[Claim 23]
To a computer which controls a distribution control device which manages delivery of goods according to a request from an order control device which manages an order received of goods
Merchandise information containing identification information of said goods, User Information about the order Lord of said goods, A reception-control step which controls reception of said delivery request information including said merchandise information, said User Information, and signature information corresponding to said successful-bidder information which were generated using a secret key managed by successful-bidder information about an administrator of said order control device, and said order control device,
A request step which controls transmission to a certificate authority of said successful-bidder information, and requires transmission of a public key corresponding to said secret key,
Verification steps which verify the justification of said signature information using said public key transmitted from said certificate authority according to a demand by processing of said request step,
A storage control step which makes an information management chip delivered with said goods memorize delivery pertinent information about delivery of said goods when the justification of said signature information is checked by processing of said

verification steps
A program making it perform.
[Claim 24]
In an information management chip delivered with goods,
A memory measure which memorizes a secret key,
A reception means which receives random information transmitted via short-distance-radio communication from an information processor operated by recipient of said goods,
The 1st creating means that generates the 1st signature information corresponding to said random information received by said reception means using said secret key memorized by said memory measure,
The 1st transmitting means that transmits said 1st signature information generated by said 1st creating means to said information processor via said short-distance-radio communication
An information management chip characterized by preparation ******.
[Claim 25]
When said memory measure has memorized further delivery pertinent information about delivery of said goods,
The 2nd creating means that generates the 2nd signature information corresponding to said delivery pertinent information using said secret key,
The 2nd transmitting means that transmits said delivery pertinent information and said 2nd signature information generated by said 2nd creating means to said information processor via said short-distance-radio communication
The information management chip according to claim 24 preparing for a pan.
[Claim 26]
Merchandise information in which said memory measure contains identification information of said goods, User Information about the order Lord of said goods, Information containing at least one of successful-bidder information about an administrator of an order control device who manages an order received of said goods, and the delivery administrator information about a delivery administrator who manages delivery of said goods is memorized as said delivery pertinent information.
The information management chip according to claim 24 characterized by things.
[Claim 27]
In an information management method of an information management chip delivered with goods,
A memory step which memorizes a secret key,

A receiving step which receives random information transmitted via short-distance-radio communication from an information processor operated by recipient of said goods,
A generation step which generates signature information corresponding to said random information received by processing of said receiving step using said secret key memorized by processing of said memory step,
A transmission step which transmits said signature information generated by processing of said generation step to said information processor via said short-distance-radio communication
****** -- an information management method characterized by things.
[Claim 28]
In a recording medium of a program which a computer which controls an information management chip delivered with goods is made to execute,
A storage control step which controls memory of a secret key,
A reception-control step which controls reception of random information transmitted via short-distance-radio communication from an information processor operated by recipient of said goods,
A generation step which generates signature information corresponding to said random information received by processing of said reception-control step using said secret key memorized by processing of said storage control step,
A transmission-control step which controls transmission to said information processor performed via said short-distance-radio communication of said signature information generated by processing of said generation step
****** -- a recording medium with which a program which a computer characterized by things can read is recorded.
[Claim 29]
To a computer which controls an information management chip delivered with goods
A storage control step which controls memory of a secret key,
A reception-control step which controls reception of random information transmitted via short-distance-radio communication from an information processor operated by recipient of said goods,
A generation step which generates signature information corresponding to said random information received by processing of said reception-control step using said secret key memorized by processing of said storage control step,
A transmission-control step which controls transmission to said information processor performed via said short-distance-radio communication of said signature

information generated by processing of said generation step
A program making it perform.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]
This invention A verification system and a method, an information processor and a method, an order control device, and a method, contents [of the load especially delivered about a distribution control device and a method, an information management chip and a method, a recording medium, and a program], and delivery origin -- or, The justification of various information about delivery of loads, such as a delivery trader, easily, And it is related with the verification system it enables it to check certainly and a method, an information processor and a method, an order control device and a method, a distribution control device and a method, an information management chip and a method, a recording medium, and a program.
[0002]
[Description of the Prior Art]
In recent years besides what is called telephone-shopping that orders by telephone the goods introduced by the Television Sub-Division program, and purchases them, The opportunity which can order favorite goods easily is increasing without the on-line shopping using the Internet etc. generally spreading, and going to a store.
[0003]
Therefore, since a close-up of various kinds of vicious incidents about the load which the opportunity to receive loads, such as goods delivered by the delivery trader, has increased, and has been delivered there was taken, for example, ******** [that the sent goods are the goods which he ordered truly, and it is not a dangerous object etc.] -- or, The importance of the distribution system which can receive goods in comfort is recognized without the person who came goods to the report feeling uneasy [whether to be the delivery trader who came to the report the goods which he ordered truly].

[0004]
For example, to the patent documents 1 mentioned later, as a distribution system which can receive goods without feeling such uneasy. The signature values (signature data) over it are remembered to be data of a product identification child, a signer identifier, a receiver identifier, etc. by the data carrier 1 (tag) stuck on goods etc. The system which enables it to check a product, a signer, a receiver, etc. by verifying the signature is indicated.

[0005]
The system which enables it to check whether goods are genuine articles is indicated by verifying the signature memorized by the tag to the patent documents 2 as a thing using the tag stuck on goods using the public key published from the authentication server 104.
[0006]
[Patent documents 1]
JP,2000-305995,A (for example, the 10th page thru/or the 12th page)
[Patent documents 2]
JP,2000-11114,A (for example, the 2nd page thru/or the 3rd page, drawing 1)
[0007]
[Problem(s) to be Solved by the Invention]
However, in the system currently indicated by the patent documents 1 and the patent documents 2, Since the signature data generated by just delivery origin is saved to the tag (data carrier) stuck on goods and verification of signature data is performed based on it, Temporarily, signature data was revealed to the third party, and when the person stored signature data in other tags and other goods were delivered, SUBJECT that the recipient could not perceive that the delivered goods are unjust occurred.
[0008]
That is, since the signature data memorized by the third party at the tag is the same as that of what is managed by just delivery origin, even if it is a case where the recipient of goods verifies the information memorized by the tag, the delivered goods will be detected as a just thing.
[0009]
This invention is made in view of such a situation, and enables it for contents [of the delivered load] and delivery origin to check easily and certainly the justification of various information about delivery of loads, such as a delivery trader.
[0010]

[Means for Solving the Problem]
This invention is characterized by an information processor which constitutes a verification system comprising the following.
An acquisition means which acquires a public key corresponding to a secret key saved by an information management chip.
A random information creating means which generates random information.
A random information transmission means which transmits generated random information to an information management chip via short-distance-radio communication.
A signature information reception means which receives signature information generated by an information management chip as a thing corresponding to random information via short-distance-radio communication, and a verifying means which verifies received signature information using an acquired public key.

[0011]
This invention is characterized by an information management chip which constitutes a verification system comprising the following.
A memory measure which memorizes a secret key.
A random information receiving means which receives random information transmitted via short-distance-radio communication from an information processor operated by recipient of goods.
A signature information creating means which generates signature information corresponding to received random information using a secret key memorized.
A signature information transmitting means which transmits generated signature information to an information processor via short-distance-radio communication.

[0012]
This invention is characterized by an information processing method which constitutes a verification method of a verification system comprising the following.
An acquisition step which acquires a public key corresponding to a secret key saved by an information management chip.
A random information generation step which generates random information.
A random transmitting information step which transmits generated random information to an information management chip via short-distance-radio communication.
A signature information receiving step which receives signature information generated

by an information management chip as a thing corresponding to random information via short-distance-radio communication, and verification steps which verify received signature information using an acquired public key.

[0013]
This invention is characterized by an information management method which constitutes a verification method of a verification system comprising the following.
A memory step which memorizes a secret key.
A random information reception step which receives random information transmitted via short-distance-radio communication from an information processor operated by recipient of goods.
A signature information generation step which generates signature information corresponding to received random information using a secret key.
A signature information transmission step which transmits generated signature information to an information processor via short-distance-radio communication.

[0014]
This invention is characterized by an information processor comprising the following.
An acquisition means which acquires a public key corresponding to the 1st secret key saved by the information management chip delivered with goods.
A random information creating means which generates random information.
A transmitting means which transmits generated random information to an information management chip via short-distance-radio communication.
A signature information reception means which receives the 1st signature information generated by an information management chip as a thing corresponding to random information via short-distance-radio communication, and the 1st verifying means that verifies the 1st received signature information using a public key.

[0015]
A delivery pertinent information reception means which receives the 2nd signature information corresponding to delivery pertinent information about delivery of goods generated by an information management chip using the 1st secret key via short-distance-radio communication with delivery pertinent information, It can have further the 2nd verifying means that verifies the 2nd received signature information using a public key. When the justification of the 2nd signature information is checked by the 2nd verifying means at this time as for a transmitting means, random

information is transmitted to an information management chip.

[0016]

When the justification of the 1st signature information is checked by the 1st verifying means, it can have further a delivery pertinent information output means which outputs delivery pertinent information.

[0017]

It can have further a verification result output means which outputs a verification result by the 1st verifying means.

[0018]

A signature information creating means which generates the 2nd signature information corresponding to merchandise information containing identification information of goods, and User Information about the order Lord of goods using the 2nd secret key remembered to be a memory measure which memorizes the 2nd secret key, Ordering information including merchandise information, User Information, and the 2nd signature information generated by signature information creating means is transmitted to an order control device which manages an order received of goods, and it can have further an order means to order goods.

[0019]

When it has been reported from an order control device that an order of goods was accepted, it can have further a request means which requires transmission of a public key corresponding to the 1st secret key from a certificate authority. At this time, an acquisition means acquires a public key transmitted from a certificate authority according to a demand by a request means.

[0020]

This invention is characterized by an information processing method of an information processor comprising the following.

An acquisition step which acquires a public key corresponding to a secret key managed by the information management chip delivered with goods.

A generation step which generates random information.

A transmission step which transmits generated random information to an information management chip via short-distance-radio communication.

A receiving step which receives signature information generated by an information management chip as a thing corresponding to random information via short-distance-radio communication, and verification steps which verify received signature information using an acquired public key.

[0021]
An acquisition control step which controls acquisition of a public key corresponding to a secret key managed by the information management chip by which the 1st recording medium of this invention has been delivered with goods, A generation step which generates random information, and a transmission-control step which controls transmission to an information management chip performed via short-distance-radio communication of generated random information, A reception-control step which controls reception performed via short-distance-radio communication of signature information generated by an information management chip as a thing corresponding to random information, A program which a computer containing verification steps which verify received signature information using a public key can read is recorded.
[0022]
The 1st program of this invention to a computer which controls an information processor which verifies the justification of delivered goods. An acquisition control step which controls acquisition of a public key corresponding to a secret key managed by the information management chip delivered with goods, A generation step which generates random information, and a transmission-control step which controls transmission to an information management chip performed via short-distance-radio communication of generated random information, A computer is made to perform a reception-control step which controls reception performed via short-distance-radio communication of signature information generated by an information management chip as a thing corresponding to random information, and verification steps which verify received signature information using a public key.
[0023]
merchandise information in which an order control device of this invention contains identification information of goods -- and, A reception means which receives ordering information including the 1st signature information corresponding to merchandise information and User Information generated using User Information about the order Lord of goods, and the 1st secret key saved by an information processor, A request means which transmits User Information to a certificate authority and requires transmission of a public key corresponding to the 1st secret key, It has a verifying means which verifies the justification of the 1st signature information using a public key transmitted from a certificate authority according to a demand by a request means, and a reporting means which notifies an information processor that an order was materialized when the justification of the 1st signature information is checked.
[0024]

A memory measure which memorizes the 2nd secret key, and a creating means which generates the 2nd signature information corresponding to merchandise information, User Information, and successful-bidder information about an administrator of an order control device using the 2nd secret key memorized, Delivery request information including merchandise information, User Information, successful-bidder information, and the 2nd signature information generated by creating means is transmitted to a distribution control device which manages delivery of goods, and it can have further a delivery request means to request delivery of goods.

[0025]

Merchandise information in which an order-receiving-control method of an order control device of this invention contains identification information of goods, And a receiving step which was generated using User Information about the order Lord of goods, and a secret key saved by an information processor and which receives merchandise information and ordering information including signature information corresponding to User Information, A request step which transmits User Information to a certificate authority and requires transmission of a public key corresponding to a secret key, Verification steps which verify the justification of signature information using a public key transmitted from a certificate authority according to a demand, and a notification step which notifies an information processor that an order was materialized when the justification of signature information is checked are included.

[0026]

merchandise information in which the 2nd recording medium of this invention contains identification information of goods -- and, A reception-control step which was generated using User Information about the order Lord of goods, and a secret key saved by an information processor and which controls reception of merchandise information and ordering information including signature information corresponding to User Information, A request step which controls transmission to a certificate authority of User Information, and requires transmission of a public key corresponding to a secret key, When verification steps which verify the justification of signature information, and the justification of signature information are checked using a public key transmitted from a certificate authority according to a demand, A program which a computer containing a notification control step which controls a notice to an information processor of an order having been materialized can read is recorded.

[0027]

merchandise information in which the 2nd program of this invention contains identification information of goods -- and, A reception-control step which was

generated using User Information about the order Lord of goods, and a secret key saved by an information processor and which controls reception of merchandise information and ordering information including signature information corresponding to User Information, A request step which controls transmission to a certificate authority of User Information, and requires transmission of a public key corresponding to a secret key, When verification steps which verify the justification of signature information, and the justification of signature information are checked using a public key transmitted from a certificate authority according to a demand, a notification control step and a computer which control a notice to an information processor of an order having been materialized are performed.

[0028]

This invention is characterized by a distribution control device comprising the following.

A reception means which receives delivery request information including merchandise information, User Information, and signature information corresponding to successful-bidder information which were generated using a secret key saved by merchandise information containing identification information of goods, User Information about the order Lord of goods, successful-bidder information about an administrator of an order control device, and an order control device.

A request means which transmits successful-bidder information to a certificate authority, and requires transmission of a public key corresponding to a secret key.

A verifying means which verifies the justification of signature information using a public key transmitted from a certificate authority according to a demand.

A storage control means which makes an information management chip delivered with goods memorize delivery pertinent information about delivery of goods when the justification of signature information is checked.

[0029]

It can have further a delivering means which delivers an information management chip with goods.

[0030]

At least one information on merchandise information, User Information, successful-bidder information, and delivery administrator information about a delivery administrator who manages delivery of goods can be included in delivery pertinent information.

[0031]

An information management chip can be delivered with goods, when held by distribution company who is stuck on the surface of goods, or delivers goods.

[0032]

This invention is characterized by a delivery management method of a distribution control device comprising the following.

Merchandise information containing identification information of goods, User Information about the order Lord of goods, A receiving step which receives delivery request information including merchandise information, User Information, and signature information corresponding to successful-bidder information which were generated using a secret key saved by successful-bidder information about an administrator of an order control device, and an order control device.

A request step which transmits successful-bidder information to a certificate authority, and requires transmission of a public key corresponding to a secret key.

Verification steps which verify the justification of signature information using a public key transmitted from a certificate authority according to a demand.

A storage control step which makes an information management chip delivered with goods memorize delivery pertinent information about delivery of goods when the justification of signature information is checked.

[0033]

Merchandise information in which the 3rd recording medium of this invention contains identification information of goods, User Information about the order Lord of goods, . Were generated using a secret key saved by successful-bidder information about an administrator of an order control device, and an order control device. A reception-control step which controls reception of delivery request information including merchandise information, User Information, and signature information corresponding to successful-bidder information, A request step which controls transmission to a certificate authority of successful-bidder information, and requires transmission of a public key corresponding to a secret key, When verification steps which verify the justification of signature information, and the justification of signature information are checked using a public key transmitted from a certificate authority according to a demand, A program which a computer which contains a storage control step which makes delivery pertinent information about delivery of goods memorize in an information management chip delivered with goods can read is recorded.

[0034]

Merchandise information in which the 3rd program of this invention contains

identification information of goods, User Information about the order Lord of goods, . Were generated using a secret key saved by successful-bidder information about an administrator of an order control device, and an order control device. A reception-control step which controls reception of delivery request information including merchandise information, User Information, and signature information corresponding to successful-bidder information, A request step which controls transmission to a certificate authority of successful-bidder information, and requires transmission of a public key corresponding to a secret key, When verification steps which verify the justification of signature information, and the justification of signature information are checked using a public key transmitted from a certificate authority according to a demand, A computer is made to perform a storage control step which makes an information management chip delivered with goods memorize delivery pertinent information about delivery of goods.

[0035]

This invention is characterized by an information management chip comprising the following.

A memory measure which memorizes a secret key.

A reception means which receives random information transmitted via short-distance-radio communication from an information processor operated by recipient of goods.

The 1st creating means that generates the 1st signature information corresponding to random information using a secret key.

The 1st transmitting means that transmits the 1st generated signature information to an information processor via short-distance-radio communication.

[0036]

The 2nd creating means that generates the 2nd signature information corresponding to delivery pertinent information using a secret key when a memory measure has memorized delivery pertinent information about delivery of goods further, It can have further the 2nd transmitting means that transmits delivery pertinent information and the 2nd signature information generated by the 2nd creating means to an information processor via short-distance-radio communication.

[0037]

Merchandise information in which a memory measure contains identification information of goods, User Information about the order Lord of goods, Information containing at least one of successful-bidder information about an administrator of an

order control device who manages an order received of goods, and the delivery administrator information about a delivery administrator who manages delivery of goods can be memorized as delivery pertinent information.

[0038]

This invention is characterized by an information management method of an information management chip comprising the following.

A memory step which memorizes a secret key.

A receiving step which receives random information transmitted via short-distance-radio communication from an information processor operated by recipient of goods.

A generation step which generates signature information corresponding to received random information using a secret key.

A transmission step which transmits generated signature information to an information processor via short-distance-radio communication.

[0039]

A storage control step by which the 4th recording medium of this invention controls memory of a secret key, A reception-control step which controls reception of random information transmitted via short-distance-radio communication from an information processor operated by recipient of goods, A generation step which generates signature information corresponding to received random information using a secret key, A program which a computer containing a transmission-control step which controls transmission to an information processor performed via short-distance-radio communication of generated signature information can read is recorded.

[0040]

A storage control step by which the 4th program of this invention controls memory of a secret key, A reception-control step which controls reception of random information transmitted via short-distance-radio communication from an information processor operated by recipient of goods, A computer is made to perform a generation step which generates signature information corresponding to received random information, and a transmission-control step which controls transmission to an information processor performed via short-distance-radio communication of generated signature information using a secret key.

[0041]

In a verification system and a method of this invention, a public key corresponding to a secret key managed by an information management chip is acquired, random

information is generated and generated random information is transmitted to an information management chip via short-distance-radio communication. It is received via short-distance-radio communication, and signature information generated by an information management chip as a thing corresponding to random information is verified using an acquired public key.

[0042]

From an information processor which a secret key is memorized and is operated by recipient of goods in a verification system of this invention. Signature information corresponding to random information which random information transmitted via short-distance-radio communication was received, and was received using a secret key memorized is generated, and generated signature information is transmitted to an information processor via short-distance-radio communication.

[0043]

In an information processor of this invention, a method, and a program, a public key corresponding to a secret key saved by the information management chip delivered with goods is acquired, and random information is generated. Generated random information is transmitted to an information management chip via short-distance-radio communication, it is received via short-distance-radio communication, and signature information generated as a thing corresponding to random information by an information management chip is verified using a public key.

[0044]

In an order control device of this invention, a method, and a program, Merchandise information containing identification information of goods, and User Information about the order Lord of goods, And ordering information including the 1st signature information corresponding to merchandise information and User Information generated using the 1st secret key saved by an information processor is received, User Information is transmitted to a certificate authority, and transmission of a public key corresponding to the 1st secret key is required. An information processor is notified that an order was materialized, when the justification of the 1st signature information is verified and the justification of the 1st signature information is checked using a public key transmitted from a certificate authority according to a demand.

[0045]

In a distribution control device of this invention, a method, and a program, Merchandise information containing identification information of goods, User Information about the order Lord of goods, . Were generated using a secret key saved by successful-bidder information about an administrator of an order control device,

and an order control device. Delivery request information including merchandise information, User Information, and signature information corresponding to successful-bidder information is received, and transmission of a public key corresponding to a secret key in transmission is required of a certificate authority in successful-bidder information. When the justification of signature information is verified and the justification of signature information is checked using a public key transmitted from a certificate authority according to a demand, delivery pertinent information about delivery of goods is memorized by information management chip delivered with goods.

[0046]

In an information management chip of this invention, a method, and a program, a secret key is memorized and random information transmitted via short-distance-radio communication is received from an information processor operated by recipient of goods. Using a secret key, the 1st signature information corresponding to random information is generated, and the 1st generated signature information is transmitted to an information processor via short-distance-radio communication.

[0047]

[Embodiment of the Invention]

Drawing 1 is a figure showing the example of composition of the delivering-goods system which applied this invention.

[0048]

Fundamentally the delivering-goods system which applied this invention The user terminal 1 (information processor), It comprises the maker's terminal 2, the delivery trader terminal 3, and the certificate authority (CA (Certification Authority)) 4, and transmission and reception of various kinds of information between these are performed via networks, such as the Internet.

[0049]

The user terminal 1 is operated by the user who is a consumer of goods, and when accessing the shopping site (website) which sells goods is directed, it displays the screen of a shopping site based on the data accessed and downloaded according to the directions. When it is directed that the user terminal 1 orders the goods currently sold in the shopping site, Using the secret key which he has managed, the signature information corresponding to the merchandise information about the goods to purchase and User Information about the user who is the order Lord is generated, and the generated signature information is transmitted to the maker's terminal 2 as ordering information with merchandise information and User Information. In this

example, a shopping site is managed with the maker's terminal 2, and the order received of goods is managed.

[0050]

It is contained in ordering information, and the information showing the information which identifies the goods to order, for example, the number to order, a price, etc. is included in the merchandise information transmitted to the maker's terminal 2, and, on the other hand, the information showing the name of the information and the order Lord who specify the address for delivery, a telephone number, the method of paying, etc. is included in User Information.

[0051]

When ordering information has been transmitted from the user terminal 1, the maker's terminal 2 transmits User Information included in ordering information to a certificate authority, and requires transmission of the public key (public key corresponding to the secret key managed with the user terminal 1) beforehand registered by the user. When the public key has been transmitted according to the demand, the maker's terminal 2, The signature information included in the ordering information transmitted from the user terminal 1 is verified using a public key, and it is checked whether whether neither alteration nor excision being performed by the third party to ordering information (User Information and merchandise information) and information are just.

[0052]

In drawing 1, the demand of a public key performed between the certificate authorities 4 and transmission of the public key to it are expressed by the dashed dotted line, and transmission and reception of the information between each terminal of the user terminal 1, the maker's terminal 2, and the delivery trader terminal 3 are expressed by the solid line.

[0053]

When it judges with the maker's terminal 2 having checked the justification of the ordering information transmitted from the user terminal 1 as a result of verification of signature information, The delivery trader notification information which generates the signature information corresponding to the delivery trader information which is information about the delivery trader who delivers goods, and includes the generated signature information and delivery trader information is transmitted to the user terminal 1 using the secret key which he manages that it should be notified to the user terminal 1 that the order was accepted.

[0054]

For example, the information showing the name of the establishment in the

neighborhood of a delivery trader's name, a contact, and the address for delivery specified by the user, a distribution time belt, etc. is included in delivery trader information.

[0055]

The user terminal 1 which received delivery trader notification information, The public key beforehand registered by the administrator (maker) of the maker's terminal 2 to the certificate authority 4, Transmission of the public key beforehand registered by the administrator (delivery trader) of the delivery trader terminal 3 is required, and the delivery trader notification information transmitted from the maker's terminal 2 is verified using the transmitted public key (public key of a maker).

[0056]

When judged with the transmitted delivery trader notification information being just as a result of verification, the user terminal 1 is saved at the storage parts store which builds in a delivery trader's public key acquired from the certificate authority 4. In the verification processing of signature information performed between the PKI (Public Key Infrastructure) chips 5 delivered by the delivery trader with goods (goods 6), a delivery trader's saved public key is used so that it may mention later.

[0057]

The maker's terminal 2 transmits delivery request information to the delivery trader terminal 3 that delivery of the goods ordered by the user should be requested while transmitting delivery trader notification information to the user terminal 1.

[0058]

The merchandise information, User Information, and the signature information corresponding to maker information which were generated using the secret key managed with the maker's terminal 2 other than maker information including the information showing merchandise information, User Information, a name, an address of a maker, etc. are included in delivery request information.

[0059]

When delivery request information has been transmitted from the maker's terminal 2, the delivery trader terminal 3 requires transmission of the public key beforehand registered by the maker to the certificate authority 4 that the justification should be checked, and verifies the signature information included in delivery request information using the public key transmitted according to a demand.

[0060]

When it is able to check that the alteration etc. are not given to delivery request information, the delivery trader terminal 3, The distribution company who delivers the

goods 6 (goods ordered by the user of the user terminal 1) is chosen, and the PKI chip 5 allocated by the ID card which the distribution company has is made to memorize the information relevant to delivery of merchandise information, User Information, maker information, etc. which are included in delivery request information.

[0061]

A distribution company delivers the goods 6 to the specified address for delivery, and shows it his own ID card to the user as a recipient who receives. A user makes the reader writer provided in the user terminal 1 approach the ID card (PKI chip 5) to which it was shown, and checks the justification of the information memorized by the PKI chip 5, i.e., the justification of the goods 6, using a delivery trader's public key beforehand acquired from the certificate authority 4.

[0062]

The result of verification performed between the PKI chips 5 with the user terminal 1, When it is outputted to the user terminal 1, for example, justification is not able to be checked, When the message to which it urges stopping the taking over of goods is displayed and the justification of information is able to be checked on the other hand, Based on the merchandise information, the maker information, and User Information which are memorized by the PKI chip 5, the information showing the contents of the load, the information showing a delivering agency, and the information showing the user itself who is the order Lord are displayed, respectively. The message etc. which report that goods can be taken over safely are displayed on the indicator of the user terminal 1.

[0063]

As mentioned above, since transmission and reception of various kinds of information are performed through verification of what is called PKI which verifies each time the signature information generated at the transmitting agency using the public key published from the certificate authority 4, The unjust information to which alteration, excision, etc. were performed by the third party can be prevented from being memorized by the PKI chip 5.

[0064]

therefore, since the information which has reliability in the PKI chip 5 delivered with goods will be memorized, a user trusts the verification result performed between the PKI chips 5 outputted to the user terminal 1, and he receives goods in comfort -- things can be carried out. For example, when it is what cannot trust the information memorized by the PKI chip 5, the case where the verification result displayed on the user terminal 1 is not right may happen, but such a thing can be controlled.

[0065]
Verification of signature information performed between the user terminal 1 and the PKI chip 5 so that it may mention later, Since it is performed by the signature information generated based on the then selected random number, a more positive verification result can be obtained compared with the case where it verifies for example, in the stage which delivers goods only based on the signature information memorized by the PKI chip 5 with the delivery trader terminal 3.
[0066]
Above, although the PKI chip 5 assumed that it is allocated independently [the goods 6] by the ID card which a distribution company presents, a user can be provided with it with various gestalten, such as being stuck on the position of the surface of the goods 6, for example.
[0067]
Next, each composition of the user terminal 1 of drawing 1, the maker's terminal 2, the delivery trader terminal 3, the certificate authority 4, and the PKI chip 5 is explained.
[0068]
Drawing 2 is a block diagram showing the example of composition of the user terminal 1 of drawing 1.
[0069]
A program CPU(Central Processing Unit) 11 is remembered to be by ROM(Read Only Memory) 12, Or according to the program loaded to RAM(Random Access Memory) 13, various kinds of processings are performed from the storage parts store 18. To RAM13, CPU11 performs various kinds of processings again, and also required data etc. are memorized suitably.
[0070]
CPU11, ROM12, and RAM13 are mutually connected via the bus 14. The input/output interface 15 is also connected to this bus 14 again.
[0071]
The input part 16, CRT (Cathode Ray Tube) which become the input/output interface 15 from a keyboard, a mouse, etc., The communications department 19 which comprises the storage parts store 18 which comprises the outputting part 17 which consists of a display which consists of LCD (Liquid Crystal Display) etc., a loudspeaker, etc., a hard disk, etc., a modem, etc. is connected. The communications department 19 performs various kinds of communications between the maker's terminal 2 and the certificate authority 4 via a network.
[0072]

The reader writer 20 radiates electromagnetic waves from the antenna which is not illustrated based on the control from CPU11, and when the PKI chip 5 driven using the induction electric power produced by receiving electromagnetic waves is detected nearby (range which electromagnetic waves reach), various kinds of information is transmitted [reader writer] and received between the PKI chips 5.

[0073]

The drive 21 is connected to the input/output interface 15 again if needed, The computer program which it was suitably equipped with the magnetic disk 22, the optical disc 23, the magneto-optical disc 24, or the semiconductor memory 25, and was read is installed in the storage parts store 18 if needed.

[0074]

As shown by the dashed dotted line, the user's secret key (K_{pri} (user)) is memorized by the storage parts store 18. In using the distribution system shown in drawing 1, a user requests issue of a public key from the certificate authority 4, and is making the secret key corresponding to the public key save at the user terminal 1.

[0075]

Drawing 3 is a block diagram showing the example of composition of the maker's terminal 2 of drawing 1.

[0076]

As shown in drawing 3, the maker's terminal 2 has the same composition fundamentally except for the point that the reader writer is not provided, with the user terminal 1 shown in drawing 2. About the portion which overlaps with what was mentioned above, the detailed explanation is omitted suitably.

[0077]

The maker's terminal 2 is managed by the administrator of a maker, and as shown by the dashed dotted line, the secret key (K_{pri} (maker)) of the maker is memorized by the storage parts store 38. In receiving an order using the distribution system shown in drawing 1, and delivering goods, a maker requests issue of a public key from the certificate authority 4, and is making the secret key corresponding to the public key save at the maker's terminal 2.

[0078]

Drawing 4 is a block diagram showing the example of composition of the delivery trader terminal 3 of drawing 1.

[0079]

Since it has the composition as the user terminal 1 fundamentally shown in drawing 2 also with the same delivery trader terminal 3, about the overlapping portion, detailed

explanation is omitted suitably.

[0080]

As shown by the dashed dotted line, the delivery trader's secret key (K_{pri} (delivery trader)) is memorized by the storage parts store 58 of the delivery trader terminal 3. Before a delivery trader receives a request of delivery from a maker with the distribution system shown in drawing 1 and delivers goods according to a request, he requests issue of a public key from the certificate authority 4, and is making the secret key corresponding to the public key save to the delivery trader terminal 3.

[0081]

When the PKI chip 5 which radiates electromagnetic waves based on the control from CPU51, for example, is delivered by the address for delivery with goods approaches, the reader writer 60 transmits to the PKI chip 5, and makes merchandise information, maker information, and User Information memorize via the electromagnetic waves to radiate.

[0082]

Drawing 5 is a block diagram showing the example of composition of the PKI chip 5.

[0083]

CPU81 is driven with the electric power supplied from the power supplying part 85, develops the control program memorized by ROM to RAM (neither is illustrated), and controls operation of the PKI chip 5 whole according to the developed control program. For example, CPU81 makes those information save in the memory 84 (when merchandise information, maker information, and User Information have been supplied via the communications department 82), when memorizing merchandise information, maker information, and User Information is directed from the reader writer 60 of the delivery trader terminal 3.

[0084]

The communications department 82 does envelope detection of the modulated wave (electromagnetic waves) received in the loop antenna, gets over, and outputs the data after a recovery to CPU81. The communications department 82 corresponds to the data supplied from CPU81, when transmitting signature information etc. to the reader writer 20 of the user terminal 1, For example, only when a switching element is an ON state, by connecting predetermined load in parallel with a loop antenna, make a predetermined switching element turn on and off, make load change it, and by the change. The electromagnetic waves from the reader writer 20 are modulated, and the modulation components are transmitted to the reader writer 20.

[0085]

As for the information transmitted to the reader writer 20, in the operation part 83, encryption is suitably given according to a prescribed method from the communications department 82.

[0086]

The operation part 83 generates the signature information corresponding to it using the secret key saved in the memory 84, when signature information is generated based on the control from CPU81, for example, the random number of a predetermined digit number has been transmitted from the reader writer 20 of the user terminal 1. The generated signature information is transmitted to the reader writer 20 via the communications department 82.

[0087]

The secret key (K_{pri} (delivery trader)) which the memory 84 is constituted from a nonvolatile memory, for example, a delivery trader manages is saved. The secret key (K_{pri} (delivery trader)) memorized by the memory 84 is supplied to the operation part 83 via CPU81, and is used in generation of signature information. As mentioned above, the public key corresponding to the secret key saved in the memory 84 is distributed from the certificate authority 4.

[0088]

After the power supplying part 85 rectifies the alternating current magnetic field excited in the loop antenna and stabilizes it, it is supplied to each part of the PKI chip 5 as DC power supply. The electric power of the electromagnetic waves radiated from the reader writer 20 or the reader writer 60 is adjusted so that the magnetic field which provides electric power required for the PKI chip 5 may be generated.

[0089]

In the public key cryptosystem which explanation used for convenience, for example, used a RSA cryptosystem, an elliptic curve cryptosystem system, etc., the "PKI chip" expresses generation of a signature, and IC (information management chip) which performs the verification by hardware.

[0090]

Drawing 6 is a block diagram showing the example of composition of the certificate authority 4.

[0091]

The certificate authority 4 also has the same composition fundamentally with the user terminal 1 and the maker's terminal 2 which were mentioned above, and the delivery trader terminal 3.

[0092]

The public key corresponding to the secret key managed with the user terminal 1 by the storage parts store 108 ($K_{plutoniumb}$ (user)), The public key (K_{pub} (maker)) corresponding to the secret key managed with the maker's terminal 2 and the public key (K_{pub} (delivery trader)) corresponding to the secret key managed with the delivery trader terminal 3 are saved.

[0093]

In the distribution system of drawing 1, CPU101, According to the demand from the user terminal 1, the public key registered by the maker and the public key registered by the delivery trader are provided via the communications department 109, and the public key registered by the user is provided according to the demand from the maker's terminal 2. CPU101 provides the public key registered by the maker according to the demand from the delivery trader terminal 3 via the communications department 109.

[0094]

Next, operation of the distribution system of drawing 1 is explained with reference to a flow chart.

[0095]

With reference to the flow chart of introduction and drawing 7, the order processing of the user terminal 1 which orders goods to the maker's terminal 2 is explained.

[0096]

In Step S1, CPU11 of the user terminal 1 accesses the shopping site which a maker manages according to the directions from a user, and displays the screen of a shopping site on the indicator which constitutes the outputting part 17.

[0097]

In Step S2, CPU11 stands by until it judges whether the order of goods was directed by the user and judges with an order having been placed based on the output from the input part 16. For example, when ending access to a shopping site is directed by the user, without ordering goods, the processing shown in drawing 7 is ended.

[0098]

In Step S2, CPU11 out of the goods currently sold in the shopping site. When it judges with the order of predetermined goods having been directed, it progresses to Step S3 and the signature information corresponding to merchandise information and User Information is generated using the secret key (K_{pri} (user)) memorized by the storage parts store 18.

[0099]

The merchandise information which specifically includes the information showing the

number etc. which place an order for CPU11 with the identification information of the goods in which the order was directed, And User Information including the information showing a user's name, the address for delivery, a telephone number, a mail address, the method of paying, etc. is acquired based on the input from a user, and a hash function is applied to the merchandise information and User Information which were acquired. CPU11 makes signature information the encryption data obtained by enciphering the message digest obtained with the application of the hash function using a secret key.

[0100]

In step S4, CPU11 controls the communications department 19 and transmits ordering information including merchandise information, User Information, and the signature information generated at Step S3 to the maker's terminal 2 which manages an order received of goods via a network.

[0101]

Next, with reference to the flow chart of drawing 8, the processing order of the maker's terminal 2 performed corresponding to processing of drawing 7 is explained.

[0102]

In Step S11, CPU31 of the maker's terminal 2 stands by until it judges whether ordering information has been transmitted from the user terminal 1 based on the output from the communications department 39 and judges with ordering information having been transmitted.

[0103]

In Step S11, when it judges with ordering information having been transmitted, it progresses to Step S12, and CPU31 controls the communications department 39, and receives ordering information. In Step S13, CPU31 transmits User Information included in ordering information to the certificate authority 4, and requires transmission of the public key (certificate) corresponding to the secret key managed with the user terminal 1.

[0104]

When a check of the maker which demands issue of a public key is performed between the maker's terminal 2 and the certificate authority 4 if needed and a check of a maker is completed, The certificate containing the public key (K_{pub} (user)) corresponding to the secret key (K_{pri} (user)) managed with the user terminal 1 is transmitted.

[0105]

In Step S14, CPU31 stands by until it judges whether the certificate has been transmitted from the certificate authority 4 and judges with having been transmitted

based on the output from the communications department 39.

[0106]

In Step S14, when it judges with the certificate which contains a public key from the certificate authority 4 having been transmitted, it progresses to Step S15, and CPU31 receives it (acquiring) and follows it to Step S16.

[0107]

In Step S16, CPU31 applies a hash function to the merchandise information and User Information which are included in ordering information, and generates a message digest (MD). In Step S17, CPU31 decodes the signature information (signature information generated in Step S3 of drawing 7) included in ordering information using the public key contained in a certificate, and generates a message digest.

[0108]

In Step S18, CPU31 compares the message digest generated at Step S16 with the message digest generated at Step S17, and judges whether they are in agreement. When judged with two message digests not being in agreement, i.e., changing with these judgments, it, It means that there is a possibility that the alteration etc. might be given by the third party to ordering information and User Information, and when judged with two message digests being in agreement on the other hand, an alteration etc. are not given to User Information and merchandise information, but it expresses that it is reliable information to them.

[0109]

Therefore, the message digest which generated CPU31 at Step S16 in Step S18, When it judges with the message digest generated at Step S17 not being in agreement, it progresses to Step S19, the message which cannot accept an order and which gives a thing notice is transmitted to the user terminal 1, and processing is terminated after that.

[0110]

On the other hand in Step S18, CPU31, Since it is what can trust an order when it judges with the message digest generated at Step S16 and the message digest generated at Step S17 being in agreement, It progresses to Step S20 and the signature information corresponding to delivery trader information is generated using the secret key (K_{pri} (maker)) memorized by the storage parts store 38 that a user should be notified of the information about a delivery trader.

[0111]

The establishment which is in delivery trader information in a delivery trader's name and the neighborhood of the specified address for delivery, The information showing

the time of a delivery date, etc. is included, and it is generated based on the ordering information transmitted from the user terminal 1, and the information managed in a delivery trader's database currently built by the storage parts store 38. Specifically, CPU31 makes signature information the encryption data obtained by applying a hash function to delivery trader information, and enciphering the generated message digest with a secret key (K_{pri} (maker)) in Step S20.

[0112]

In Step S21, CPU31 transmits delivery trader notification information including delivery trader information and the signature information generated at Step S20 to the user terminal 1 via the communications department 39, and reports that the order was accepted.

[0113]

Ordering information will be received only when judged with the ordering information transmitted from the user to the maker by the above processing based on the signature information generated in the user terminal 1 being just. That is, an order of inaccurate goods will be controlled.

[0114]

Next, with reference to the flow chart of drawing 9, processing of the user terminal 1 in which it is verified whether the delivery trader notification information transmitted by processing of drawing 8 from the maker's terminal 2 is just is explained.

[0115]

In Step S31, CPU11 of the user terminal 1 judges whether it has been reported from the maker's terminal 2 that the order was accepted. As mentioned above, when it is judged in the maker's terminal 2 whether it is the information which can trust ordering information and it is judged with it being reliable information, it is reported to the user terminal 1 that the order was accepted (Step S21 of drawing 8).

[0116]

. CPU11 in Step S31, it is not reported that the order was accepted. That is, when it is judged with ordering information being inaccurate with the maker's terminal 2 and judges with it having been reported that an order is unreceivable, it progresses to Step S32 and error handling is performed.

[0117]

For example, the message which notifies the purport it has been transmitted from the maker's terminal 2 that an order is unreceivable, as error handling is displayed on the outputting part 17, and a user is shown it. Then, processing is ended.

[0118]

On the other hand, in Step S31, when it judges with it having been reported that goods were received, it progresses to Step S33, and CPU11 controls the communications department 19, and receives delivery trader notification information.

[0119]

The public key (K_{pub} (maker)) corresponding to the secret key (K_{pri} (maker)) which CPU11 transmits maker information and delivery trader information to the certificate authority 4 in Step S34, and is managed with the maker's terminal 2, Transmission of the public key (K_{pub} (delivery trader)) corresponding to the secret key (K_{pri} (delivery trader)) managed with the delivery trader terminal 3 is required.

[0120]

According to this demand, a public key (K_{pub} (maker), K_{pub} (delivery trader)) is read from the database currently built by the storage parts store 108 in the certificate authority 4, and the certificate containing them is transmitted to the user terminal 1.

[0121]

In Step S35, CPU11 stands by until it judges with the certificate having been transmitted, and when it judges with the certificate having been transmitted, it progresses to Step S36 and it receives it.

[0122]

In Step S37, that it should be verified whether the delivery trader information included in the delivery trader notification information transmitted from the maker's terminal 2 is just, CPU11 applies a hash function to delivery trader information, and generates a message digest. In Step S38, CPU11 decodes signature information (signature information which was enciphered with the secret key (K_{pri} (maker)) and was generated in the maker's terminal 2) using the public key (K_{pub} (maker)) contained in a certificate, and generates a message digest.

[0123]

CPU11 compares the message digest generated at Step S37 with the message digest generated at Step S38 in Step S39, and judges whether those message digests are in agreement.

[0124]

When judged with the message digest generated at Step S37 and the message digest generated at Step S38 not being in agreement in Step S39, it, Since it expresses that it is the information which cannot trust delivery trader information, it progresses to Step S32 and CPU11 performs error handling. For example, in Step S32, since CPU11 has a possibility that delivery trader information may be unjust information, it displays the message which reports that an order of goods is stopped.

[0125]
When judged with the message digest generated at Step S37 and the message digest generated at Step S38 being in agreement, on the other hand in Step S39, it, Since it expresses that it is the information which can trust the delivery trader notification information transmitted from the maker's terminal 2, CPU11, It progresses to Step S40, and while showing a user the information (information at the time of a delivery trader name and a delivery date, etc.) about the delivery trader of the schedule which delivers goods, the public key (K_{pub} (delivery trader)) transmitted from the certificate authority 4 is made to save at the storage parts store 18.
[0126]
In the verification processing performed between the PKI chips 5 delivered with goods, the public key (K_{pub} (delivery trader)) saved at the storage parts store 18 is used, when goods have actually been delivered.
[0127]
As mentioned above, the information notified from the maker's terminal 2 as information about the delivery trader who delivers goods, Only when it verifies using the public key corresponding to the secret key managed with the maker's terminal 2 and it is detected that it is just, that it was made to continue order processing A sake, The information at the time of a delivery trader's name shown to the user or a delivery date, etc. turns into reliable information to which the alteration etc. are not given by the third party. That is, the user can check that goods are delivered from the delivery trader formally requested by the maker.
[0128]
Next, with reference to the flow chart of drawing 10, processing of the maker's terminal 2 in which delivery of goods is requested to a delivery trader is explained. This processing is performed following the processing shown in drawing 8, for example.
[0129]
In Step S51, CPU31 of the maker's terminal 2, The signature information corresponding to maker information including the information showing the merchandise information, User Information and the manufacture name which have been transmitted from the user terminal 1, a contact, etc. is generated using the secret key (K_{pri} (maker)) saved at the storage parts store 38. For example, CPU31 enciphers the message digest obtained by applying a hash function to merchandise information, User Information, and maker information using a secret key (K_{pri} (maker)), and generates signature information.
[0130]

It progresses to Step S52, and CPU31 controls the communications department 39, and transmits delivery request information including merchandise information, User Information, maker information, and the signature information generated at Step S51 to the delivery trader terminal 3.

[0131]

Next, with reference to the flow chart of drawing 11, the delivery request confirming processing of the delivery trader terminal 3 performed corresponding to processing of drawing 10 is explained.

[0132]

In Step S61, when it judges whether delivery request information has been transmitted from the maker's terminal 2 and judges with having been transmitted, it progresses to Step S62, and CPU51 of the delivery trader terminal 3 controls the communications department 59, and receives delivery request information.

[0133]

In Step S63, CPU51 transmits the maker information included in delivery request information to the certificate authority 4, and requires transmission of the public key (K_{pub} (maker)) corresponding to the secret key (K_{pri} (maker)) managed with the maker's terminal 2.

[0134]

In the certificate authority 4, a public key (K_{pub} (maker)) is read according to the demand from the delivery trader terminal 3, and it is transmitted to the delivery trader terminal 3.

[0135]

In Step S64, CPU51 stands by until it judges whether the certificate containing a public key (K_{pub} (maker)) has been transmitted from the certificate authority 4 based on the output from the communications department 59 and judges with the certificate having been transmitted.

[0136]

In Step S64, it progresses to Step S65 and CPU51 receives it, when it judges with the certificate having been transmitted.

[0137]

In Step S66, that the justification of the delivery request information transmitted from the maker's terminal 2 should be checked, CPU51 applies a hash function to merchandise information, User Information, and maker information, and generates a message digest. Signature information by which CPU51 is contained in delivery request information in Step S67 (it is enciphered with the secret key (K_{pri} (maker))

managed with the maker's terminal 2, and) The generated signature information is decoded using the public key (K_{pub} (maker)) to which it has been transmitted from the certificate authority 4, and a message digest is generated.

[0138]

CPU51 judges whether the message digest generated at Step S66 and the message digest generated at Step S67 are in agreement in Step S68. When it judges with those message digests of CPU51 not corresponding in Step S68, it, Since there is a possibility that the alteration etc. might be given to the delivery request information transmitted from the maker's terminal 2 and it expresses that it is the information which is not reliable, it progresses to Step S69 and it is reported to the maker's terminal 2 that a request of delivery cannot be received.

[0139]

On the other hand in Step S68, CPU51, When it judges with the message digest generated at Step S66 and the message digest generated at Step S67 being in agreement, the distribution company who delivers goods is chosen as the address for delivery specified by the user from the distribution companies followed and registered into Step S70.

[0140]

CPU51 makes the PKI chip 5 currently allocated by the ID card which the distribution company selected at Step S70 has memorize User Information, merchandise information, and maker information in Step S71. When a recipient is provided with the PKI chip 5 in the form stuck on the surface of goods, the PKI chip 5 with which User Information, merchandise information, and maker information were written in is stuck on the surface of goods (goods which the user ordered).

[0141]

For example, CPU51 controls the reader writer 60, radiates electromagnetic waves, makes the PKI chip 5 (ID card) close to the reader writer 60 generate induction electric power, and makes the memory 84 memorize User Information, merchandise information, and maker information via electromagnetic waves.

[0142]

As mentioned above, since a request of delivery is received only when the justification of the delivery request information transmitted from the maker's terminal 2 is checked, Temporarily, delivery request information is altered, and even if it is a case where the information on the address for delivery is rewritten, the situation of goods being delivered by the rewritten address for delivery can be controlled. That is, only reliable User Information, merchandise information, and maker information which have been

transmitted by the system of PKI without giving an alteration etc. will be saved for the PKI chip 5.

[0143]

Next, with reference to the flow chart of drawing 12, the storage processing of the PKI chip 5 performed corresponding to processing of drawing 11 is explained.

[0144]

In Step S81, CPU81 of the PKI chip 5, It judges whether based on the output from the communications department 82, having saved User Information, merchandise information, and maker information was directed, and it stands by until those information is transmitted via the electromagnetic waves radiated from the reader writer 60 of the delivery trader terminal 3. When the electromagnetic waves radiated from the reader writer 60 are received in a loop antenna, the DC power supply generated by the power supplying part 85 based on induction electric power are supplied to each part of the PKI chip 5.

[0145]

In Step S81, CPU81 from the reader writer 60 of the delivery trader terminal 3. User Information, merchandise information, and maker information are transmitted, when saving those information judges with having been directed, it progresses to Step S82 and the memory 84 is made to memorize User Information, merchandise information, and maker information (information relevant to delivery).

[0146]

Next, with reference to the flow chart of drawing 13, processing of the certificate authority 4 which publishes a public key is explained according to the demand from the user terminal 1, the maker's terminal 2, and the delivery trader terminal 3.

[0147]

In Step S91, CPU101 of a certificate authority stands by until it judges whether issue of the public key was required and judges with issue having been required.

[0148]

CPU101 by processing of the user terminal [in / by processing of the maker's terminal 2 in Step S13 of drawing 8 / Step S34 of drawing 9] 1. Or when it judges with issue of the public key having been required by processing of the delivery trader terminal 3 in Step S63 of drawing 11, the public key demanded by progressing to Step S92 is read from the database currently built by the storage parts store 108. The read public key is published in Step S93 (transmitted).

[0149]

By the above processing, according to the demand from the user terminal 1, the public

key (K_{pub} (maker)) of a maker and a delivery trader's public key (K_{pub} (delivery trader)) are published, and a user's public key (K_{pub} (user)) is published according to the demand from the maker's terminal 2. The public key (K_{pub} (maker)) of a maker is published according to the demand from the delivery trader terminal 3.

[0150]

Next, with reference to the flow chart of drawing 14 and drawing 15, signature information is verified between the PKI chips 5 delivered with goods, and processing of the user terminal 1 in which goods are checked is explained.

[0151]

A distribution company delivers goods (ordered goods) to the address for delivery specified by the user, and according to showing a user its own ID card, this processing is performed, when a user makes the reader writer 20 of the user terminal 1 approach.

[0152]

In Step S101, CPU11 of the user terminal 1 controls the reader writer 20, and radiates the electromagnetic waves for detecting the PKI chip 5 (ID card). In Step S102, CPU11 stands by until it judges whether the PKI chip 5 was detected based on the response from the PKI chip 5 to the radiated electromagnetic waves and judges with the PKI chip 5 having been detected.

[0153]

In Step S102, when it judges with the PKI chip 5 having been detected, it progresses to Step S103, and CPU11 controls the reader writer 20, and transmits the acknowledge request of goods to the PKI chip 5.

[0154]

For example, according to an acknowledge request being received the PKI chip 5, User Information, merchandise information, and maker information which are memorized by the memory 84 -- and, In order to transmit the signature information generated with the secret key saved for the PKI chip 5 corresponding to those information (Step S134 of drawing 16), CPU11, In Step S104, it stands by until it judges whether User Information, merchandise information, maker information, and signature information have been transmitted from the PKI chip 5 and judges with having been transmitted.

[0155]

In Step S104, when it judges with User Information, merchandise information, maker information, and the signature information corresponding to those information having been transmitted, it progresses to Step S105, and CPU11 controls the reader writer 20, and receives those information (it reads).

[0156]

In Step S106, CPU11 reads the public key (K_{pub} (delivery trader)) of the delivery trader who saved beforehand at the storage parts store 18 by processing of Step S40 of drawing 9, and verifies the signature information transmitted from the PKI chip 5. That is, it progresses to Step S107, and CPU11 applies a hash function to User Information, merchandise information, and maker information which have been transmitted from the PKI chip 5, and generates a message digest.

[0157]

In Step S108, CPU11 decodes the signature information transmitted from the PKI chip 5 using the public key (K_{pub} (delivery trader)) read from the storage parts store 18, and generates a message digest.

[0158]

The message digest which generated CPU11 at Step S107 in Step S109, When it judges whether the message digest generated at Step S108 is in agreement and judges with it not being in agreement, it progresses to Step S110 and the message which notifies what the check of goods was not able to carry out is displayed. For example, a user is shown the message to which it urges stopping the receipt of goods.

[0159]

On the other hand, in Step S109, when it judges with the message digest generated at Step S107 and the message digest generated at Step S108 being in agreement, it progresses to Step S111 and CPU11 generates the random number of the predetermined digit number as random information. The generated random number is transmitted to the PKI chip 5 from the reader writer 20 in Step S112.

[0160]

In the PKI chip 5, the signature information corresponding to the random number transmitted from the user terminal 1 is generated using the secret key saved, and it is transmitted to the user terminal 1 (Step S138 of drawing 16).

[0161]

In Step S113, CPU11 stands by until it judges whether signature information has been transmitted from the PKI chip 5 and judges with having been transmitted based on the output from the reader writer 20.

[0162]

In Step S113, it progresses to Step S114 and CPU11 receives it, when it judges with the signature information corresponding to a random number having been transmitted from the PKI chip 5.

[0163]

That CPU11 should check the justification of the transmitted signature information

(signature information generated corresponding to the random number) in Step S115, While applying a hash function to the random number generated at Step S111 and generating a message digest, it progresses to Step S116, the signature information transmitted from the PKI chip 5 is decoded using a public key (K_{pub} (delivery trader)), and a message digest is generated.

[0164]

The message digest which generated CPU11 at Step S115 in Step S117, Since it progressed to Step S110 and the check of goods was not completed when it judged whether the message digest generated at Step S116 is in agreement and judged with it not being in agreement, the message which stimulates stopping the receipt of goods is displayed.

[0165]

The message digest generated at Step S115 in Step S117 on the other hand, When it judges with the message digest generated at Step S116 being in agreement, CPU11, It progresses to Step S118, the user itself places an order for the check of goods having been completed, i.e., the delivered goods, and a delivering agency displays the information showing being the maker which the user ordered goods.

[0166]

For example, CPU11 displays the name etc. of the delivered goods based on the merchandise information read from the PKI chip 5, and displays the name etc. of the maker which is the delivery origin of goods based on maker information. moreover -- being based on User Information -- an order -- the user as main -- the person's himself/herself name, an address, etc. are displayed.

[0167]

Thus, since information corresponding based on the information acquired from the PKI chip 5 is displayed, without opening goods, contents can be checked, and the user can trust and receive the delivered goods.

[0168]

Since verification is performed using the random number generated on the occasion of a receipt, a more positive judgment can be made compared with the case where the justification of goods is judged only based on the information beforehand saved for the PKI chip 5.

[0169]

Next, with reference to the flow chart of drawing 16, the confirming processing of the PKI chip 5 performed corresponding to processing of drawing 14 and drawing 15 is explained.

[0170]
In Step S131, CPU81 of the PKI chip 5 stands by until it judges whether the acknowledge request of goods has been transmitted based on the output from the communications department 82 and judges with having been transmitted. In the user terminal 1, when electromagnetic waves are radiated and the PKI chip 5 is detected from the reader writer 20 at the radiation within the limits, the acknowledge request of goods is transmitted to the PKI chip 5 (Step S103 of drawing 14).
[0171]
In Step S131, it progresses to Step S132 and CPU81 reads a secret key (K_{pri} (delivery trader)) from the memory 84, when it judges with the acknowledge request having been transmitted from the user terminal 1.
[0172]
In Step S133, CPU81 controls the operation part 83 and the secret key (K_{pri} (delivery trader)) read at Step S132 is used for it, The signature information corresponding to User Information, merchandise information, and maker information which are saved in the memory 84 is generated, and the generated signature information is transmitted to the user terminal 1 in Step S134 with User Information, merchandise information, and maker information.
[0173]
When the justification of the information which verification of the transmitted signature information is performed and is saved by the PKI chip 5 is checked, from the user terminal 1. Since the random number of a predetermined digit number is transmitted (Step S112 of drawing 15), CPU81 stands by in Step S135 until it judges whether the random number has been transmitted and judges with having been transmitted.
[0174]
In Step S135, it progresses to Step S136 and CPU81 receives it, when it judges with the random number having been transmitted.
[0175]
CPU81 transmits the signature information which generated the signature information corresponding to a random number, and was followed and generated to Step S138 to the user terminal 1 in Step S137 using the secret key (K_{pri} (delivery trader)) memorized by the memory 84.
[0176]
When verification of signature information is performed in the user terminal 1 based on the signature information transmitted in Step S138 (Step S117 of drawing 15) and it is

verified that signature information is just, The message which reports that goods are safely receivable is displayed on an indicator (Step S118 of drawing 15).

[0177]

As mentioned above, between the PKI chips 5 with which information reliable by the system of PKI was memorized, Since verification of the justification of goods is performed based on the signature information corresponding to the random number generated just before receiving goods, the user can check certainly [before opening] whether the delivered goods are the goods which he ordered truly. Since verification of the product is performed by non-contact short-distance-radio communication between the PKI chip 5 stuck on the distribution company's ID card and goods, and a reader writer, the user can make a reader writer only able to approach and can perform the verification easily.

[0178]

In the above, although an order of the goods to the maker's terminal 2 and verification of the delivered goods presupposed that it is performed by the one user terminal 1, those processings may be made to be performed by terminal different, respectively. In this case, when receiving goods, a user holds only the terminal (reader writer) in which the public key (public key corresponding to the secret key saved for the PKI chip 5) was saved, in order that he may verify the information memorized by the PKI chip 5, and receives a distribution company.

[0179]

The verification processing performed between the user terminal 1 and the PKI chip 5, If it is the radio performed for a short distance, for example, what is called wireless LAN (Local Area Network) and Bluetooth, such as IEEE(Institute of Electrical and Electronics Engineers) 802.11a or 802.11b, -- or, It can be made to perform with various communication methods, such as short distance communication by infrared rays.

[0180]

Although it presupposed at the PKI chip 5 delivered with goods above that User Information, merchandise information, and maker information are memorized, any at least one of those information may be made to be memorized. For example, when only User Information is memorized by the PKI chip 5, the user can check whether the delivered goods are the goods which he ordered truly by referring to the information displayed on the indicator of the user terminal 1 after verification of signature information. That is, when User Information to which the alteration etc. are not given is saved for the PKI chip 5, a user's own name, address, etc. which are the order Lord

will be displayed on the indicator of the user terminal 1.

[0181]

Similarly, only merchandise information is memorized by the PKI chip 5, and when it is just, to the indicator of the user terminal 1. Since the name and the number of the goods which the user itself ordered are displayed, the user can check the contents of goods before opening by referring to the information displayed.

[0182]

Since only maker information is memorized by the PKI chip 5, and the name etc. of the maker which is the orderer of goods are displayed on the indicator of the user terminal 1 when it is just, the user can check the delivery origin of goods by referring to the information displayed.

[0183]

Although the maker which manages the maker's terminal 2 above differs from the delivery trader who manages the delivery trader terminal 3, respectively, to the consumer and supplier side, change of a system configuration is possible for a maker serving as a delivery trader etc. respectively.

[0184]

When a maker serves as a delivery trader, the distribution system which applied this invention is constituted, for example, as shown in drawing 17.

[0185]

The user terminal 1 transmits ordering information including merchandise information, User Information, and the signature information (signature information which was enciphered with the secret key managed with the user terminal 1, and was generated) corresponding to those information to the maker's terminal 2, when ordering goods according to the directions from a user. The maker's terminal 2 which received ordering information requires transmission of the public key corresponding to the secret key managed in the user terminal 1 from the certificate authority 4 that the justification of ordering information should be checked, and verifies the signature information included in ordering information using the public key transmitted according to a demand.

[0186]

When the justification of ordering information is able to be checked, the maker's terminal 2 transmits order reception information to the user terminal 1, and reports that the order was accepted. The information showing the time of the delivery date corresponding to the delivery trader information in the distribution system of drawing 1, a distribution company, etc. and the signature information which was enciphered

with the secret key managed with the maker's terminal 2, and was generated corresponding to that information are included in this order reception information, for example.

[0187]

The maker's terminal 2 makes the PKI chip 5 memorize User Information, merchandise information, and maker information, and delivers the PKI chip 5 to the user terminal 1 with the goods 6.

[0188]

When order reception information has been transmitted from the maker's terminal 2 in the user terminal 1, The public key corresponding to the secret key managed in the maker's terminal 2 is acquired from the certificate authority 4, and the public key is used in the verification processing performed between the PKI chips 5 delivered with goods.

[0189]

Thus, even if it is a case where composition is changed, the user can verify easily and certainly whether the goods delivered are just.

[0190]

When a maker may be made to serve not only as a delivery trader but as the administrator of the certificate authority 4 and an order is accepted in the distribution system of drawing 17, It may be made to require that the public key corresponding to the secret key managed from the maker's terminal 2 in the maker's terminal 2 to the certificate authority 4 should be transmitted to the user terminal 1. The user terminal 1 can be made to perform verification processing of signature information between the PKI chips 5 delivered with goods also by making the public key transmitted from the certificate authority 4 according to this demand use.

[0191]

Although a series of processings mentioned above can also be performed by hardware, they can also be performed with software.

[0192]

The computer by which the program which constitutes the software is included in hardware for exclusive use when performing a series of processings with software, Or it is installed in the personal computer etc. which can perform various kinds of functions, for example, are general-purpose, etc. from a network or a recording medium by installing various kinds of programs.

[0193]

. As shown in drawing 2, this recording medium is distributed apart from a device main

frame in order to provide a user with a program. The magnetic disk 22 (a flexible disk is included) with which the program is recorded, the optical disc 23 (CD-ROM (Compact Disk-Read Only Memory).) . DVD (Digital Versatile Disk) is included. The magneto-optical disc 24 (MD (registered trademark) (Mini-Disk) is included), Or it comprises ROM12 with which it is not only constituted by the package media which consist of the semiconductor memory 25 etc., but a user is provided in the state where it was beforehand included in the device main frame and on which the program is recorded, a hard disk contained in the storage parts store 18, etc.

[0194]

In this Description, even if the processing serially performed according to an order that the step which describes the program recorded on a recording medium was indicated is not of course necessarily processed serially, it also includes a parallel target or the processing performed individually.

[0195]

In this Description, a system expresses the whole device constituted by two or more devices.

[0196]

[Effect of the Invention]

According to this invention, the justification of the delivered goods is verifiable easily and certainly.

[0197]

According to this invention, the information transmitted and received shall be reliable.

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the example of composition of the delivering-goods system which applied this invention.

[Drawing 2]It is a block diagram showing the example of composition of the user terminal of drawing 1.

[Drawing 3]It is a block diagram showing the example of composition of the maker's terminal of drawing 1.

[Drawing 4]It is a block diagram showing the example of composition of the delivery trader terminal of drawing 1.

[Drawing 5]It is a block diagram showing the example of composition of the PKI chip of drawing 1.

[Drawing 6]It is a block diagram showing the example of composition of the certificate authority of drawing 1.

[Drawing 7]It is a flow chart explaining the order processing of a user terminal.

[Drawing 8]It is a flow chart explaining the processing order of a maker's terminal performed corresponding to processing of drawing 7.
[Drawing 9]It is a flow chart explaining the verification processing of a user terminal.
[Drawing 10]It is a flow chart explaining delivery request processing of a maker's terminal.
[Drawing 11]It is a flow chart explaining the delivery request confirming processing of a delivery trader terminal performed corresponding to processing of drawing 10.
[Drawing 12]It is a flow chart explaining the storage processing of a PKI chip performed corresponding to processing of drawing 11.
[Drawing 13]It is a flow chart explaining the public key issue processing of a certificate authority.
[Drawing 14]It is a flow chart explaining the goods confirming processing of a user terminal.
[Drawing 15]It is a flow chart following drawing 14 explaining the goods confirming processing of a user terminal.
[Drawing 16]It is a flow chart explaining the confirming processing of a PKI chip performed corresponding to processing of drawing 14 and drawing 15.
[Drawing 17]It is a figure showing other examples of composition of the distribution system which applied this invention.
[Description of Notations]
1 The user terminal 1 and 2 A maker's terminal and 3 A delivery trader terminal and 4 A certificate authority, 5 PKI chip, and 6 Goods

---

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a figure showing the example of composition of the delivering-goods system which applied this invention.
[Drawing 2]It is a block diagram showing the example of composition of the user terminal of drawing 1.
[Drawing 3]It is a block diagram showing the example of composition of the maker's

terminal of drawing 1.
[Drawing 4]It is a block diagram showing the example of composition of the delivery trader terminal of drawing 1.
[Drawing 5]It is a block diagram showing the example of composition of the PKI chip of drawing 1.
[Drawing 6]It is a block diagram showing the example of composition of the certificate authority of drawing 1.
[Drawing 7]It is a flow chart explaining the order processing of a user terminal.
[Drawing 8]It is a flow chart explaining the processing order of a maker's terminal performed corresponding to processing of drawing 7.
[Drawing 9]It is a flow chart explaining the verification processing of a user terminal.
[Drawing 10]It is a flow chart explaining delivery request processing of a maker's terminal.
[Drawing 11]It is a flow chart explaining the delivery request confirming processing of a delivery trader terminal performed corresponding to processing of drawing 10.
[Drawing 12]It is a flow chart explaining the storage processing of a PKI chip performed corresponding to processing of drawing 11.
[Drawing 13]It is a flow chart explaining the public key issue processing of a certificate authority.
[Drawing 14]It is a flow chart explaining the goods confirming processing of a user terminal.
[Drawing 15]It is a flow chart following drawing 14 explaining the goods confirming processing of a user terminal.
[Drawing 16]It is a flow chart explaining the confirming processing of a PKI chip performed corresponding to processing of drawing 14 and drawing 15.
[Drawing 17]It is a figure showing other examples of composition of the distribution system which applied this invention.
[Description of Notations]
1 The user terminal 1 and 2 A maker's terminal and 3 A delivery trader terminal and 4 A certificate authority, 5 PKI chip, and 6 Goods

---

[Translation done.]

CORRECTION OR AMENDMENT

[Kind of official gazette]Printing of amendment by regulation of Patent Law Article 17 of 2
[A section Type] The 3rd Type of the part VII gate
[Publication date]Heisei 17(2005) October 27 (2005.10.27)

[Publication No.]JP,2004-88534,A (P2004-88534A)
[Date of Publication]Heisei 16(2004) March 18 (2004.3.18)
[Annual volume number] Public presentation / registration gazette 2004-011
[Application number]application for patent 2002-248108 (P2002-248108)
[The 7th edition of International Patent Classification]
H04L 9/32

B65G 61/00

G06F 17/60

G06K 17/00

[FI]
H04L 9/00 675 B

B65G 61/00 210

B65G 61/00 522

G06F 17/60 114

G06F 17/60 302 A

G06F 17/60 334

G06F 17/60 512

G06K 17/00 F

G06K 17/00 T

[Written Amendment]
[Filing date]Heisei 17(2005) August 29 (2005.8.29)
[Amendment 1]
[Document to be Amended]Description
[Item(s) to be Amended]Title of invention
[Method of Amendment]Change
[The contents of amendment]
[Title of the Invention]A verification system and a method, an information processor and a method, an order control device and a method, a distribution control device, and a method
[Amendment 2]
[Document to be Amended]Description
[Item(s) to be Amended]Claims
[Method of Amendment]Change
[The contents of amendment]
[Claim(s)]
[Claim 1]In an information processor which verifies information relevant to delivered goods, and a verification system which consists of an information management chip delivered with said goods,
Said information processor,
An acquisition means which acquires a public key corresponding to a secret key saved

by said information management chip,
A random information creating means which generates random information,
A random information transmission means which transmits said random information generated by said random information creating means to said information management chip via short-distance-radio communication,
A signature information reception means which receives signature information generated by said information management chip as a thing corresponding to said random information transmitted by said random information transmission means via said short-distance-radio communication,
A verifying means which verifies said signature information received by said signature information reception means using said public key acquired by said acquisition means
A preparation,
Said information management chip,
A memory measure which memorizes said secret key,
A random information receiving means which receives said random information transmitted via said short-distance-radio communication from said information processor operated by recipient of said goods,
A signature information creating means which generates said signature information corresponding to said random information received by said random information receiving means using said secret key memorized by said memory measure,
A signature information transmitting means which transmits said signature information generated by said signature information creating means to said information processor via said short-distance-radio communication
A verification system characterized by preparation ******.
[Claim 2]In a verification method of an information processor which verifies information relevant to delivered goods, and a verification system which consists of an information management chip delivered with said goods,
An information processing method of said information processor,
An acquisition step which acquires a public key corresponding to a secret key saved by said information management chip,
A random information generation step which generates random information,
A random transmitting information step which transmits said random information generated by processing of said random information generation step to said information management chip via short-distance-radio communication,
A signature information receiving step which receives signature information generated by said information management chip as a thing corresponding to said random

information transmitted by processing of said random transmitting information step via said short-distance-radio communication,
Verification steps which verify said signature information received by processing of said signature information receiving step using said public key acquired by processing of said acquisition step
An implication,
An information management method of said information management chip,
A memory step which memorizes said secret key,
A random information reception step which receives said random information transmitted via said short-distance-radio communication from said information processor operated by recipient of said goods,
A signature information generation step which generates said signature information corresponding to said random information received by processing of said random information reception step using said secret key memorized inside,
A signature information transmission step which transmits said signature information generated by processing of said signature information generation step to said information processor via said short-distance-radio communication
****** -- a verification method characterized by things.
[Claim 3]In an information processor which verifies information relevant to delivered goods,
An acquisition means which acquires a public key corresponding to the 1st secret key managed by the information management chip delivered with said goods,
A random information creating means which generates random information,
A transmitting means which transmits said random information generated by said random information creating means to said information management chip via short-distance-radio communication,
A signature information reception means which receives the 1st signature information generated by said information management chip as a thing corresponding to said random information transmitted by said transmitting means via said short-distance-radio communication,
The 1st verifying means that verifies said 1st signature information received by said signature information reception means using said public key acquired by said acquisition means
An information processor characterized by preparation ******.
[Claim 4]A delivery pertinent information reception means which receives the 2nd signature information corresponding to delivery pertinent information about delivery of

said goods generated by said information management chip using said 1st secret key via said short-distance-radio communication with said delivery pertinent information,
The 2nd verifying means that verifies said 2nd signature information received by said delivery pertinent information reception means using said public key
It prepares for a pan,
Said transmitting means transmits said random information to said information management chip, when the justification of said 2nd signature information is checked by said 2nd verifying means.
The information processor according to claim 3 characterized by things.
[Claim 5]It has further a verification result output means which outputs a verification result by said 1st verifying means.
The information processor according to claim 3 characterized by things.
[Claim 6]A memory measure which memorizes the 2nd secret key,
A signature information creating means which generates the 2nd signature information corresponding to merchandise information containing identification information of said goods, and User Information about the order Lord of said goods using said 2nd secret key memorized by said memory measure,
An order means to transmit ordering information including said merchandise information, said User Information, and said 2nd signature information generated by said signature information creating means to an order control device which manages an order received of said goods, and to order said goods
The information processor according to claim 3 preparing for a pan.
[Claim 7]In an information processing method of an information processor which verifies information relevant to delivered goods,
An acquisition step which acquires a public key corresponding to a secret key managed by the information management chip delivered with said goods,
A generation step which generates random information,
A transmission step which transmits said random information generated by processing of said generation step to said information management chip via short-distance-radio communication,
A receiving step which receives signature information generated by said information management chip as a thing corresponding to said random information transmitted by processing of said transmission step via said short-distance-radio communication,
Verification steps which verify said signature information received by processing of said receiving step using said public key acquired by processing of said acquisition step

****** -- an information processing method characterized by things.
[Claim 8]In an order control device which manages an order received of goods according to an order from an information processor,
Merchandise information containing identification information of said goods, and User Information about the order Lord of said goods, And a reception means which receives ordering information including the 1st signature information corresponding to said merchandise information and said User Information generated using the 1st secret key saved by said information processor from said information processor,
A request means which transmits said User Information to a certificate authority, and requires transmission of a public key corresponding to said 1st secret key,
A verifying means which verifies the justification of said 1st signature information using said public key transmitted from said certificate authority according to a demand by said request means,
A reporting means which notifies said information processor that an order was materialized when the justification of said 1st signature information is checked by said verifying means
An order control device characterized by preparation ******.
[Claim 9]In an order-receiving-control method of an order control device of managing an order received of goods according to an order from an information processor,
Merchandise information containing identification information of said goods, and User Information about the order Lord of said goods, And a receiving step which was generated using a secret key saved by said information processor and which receives said merchandise information and ordering information including signature information corresponding to said User Information from said information processor,
A request step which transmits said User Information to a certificate authority, and requires transmission of a public key corresponding to said secret key,
Verification steps which verify the justification of said signature information using said public key transmitted from said certificate authority according to a demand by processing of said request step,
A notification step which notifies said information processor that an order was materialized when the justification of said signature information is checked by processing of said verification steps
****** -- an order-receiving-control method characterized by things.
[Claim 10]In a distribution control device which manages delivery of goods according to a request from an order control device which manages an order received of goods,
Merchandise information containing identification information of said goods, User

Information about the order Lord of said goods, A reception means which receives said delivery request information including said merchandise information, said User Information, and signature information corresponding to said successful-bidder information which were generated using a secret key managed by successful-bidder information about an administrator of said order control device, and said order control device from said order control device,
A request means which transmits said successful-bidder information to a certificate authority, and requires transmission of a public key corresponding to said secret key,
A verifying means which verifies the justification of said signature information using said public key transmitted from said certificate authority according to a demand by said request means,
A storage control means which makes an information management chip delivered with said goods memorize delivery pertinent information about delivery of said goods when the justification of said signature information is checked by said verifying means
A distribution control device characterized by preparation ******.
[Claim 11]In a delivery management method of a distribution control device which manages delivery of goods according to a request from an order control device which manages an order received of goods,
Merchandise information containing identification information of said goods, User Information about the order Lord of said goods, A receiving step which receives said delivery request information including said merchandise information, said User Information, and signature information corresponding to said successful-bidder information which were generated using a secret key managed by successful-bidder information about an administrator of said order control device, and said order control device from said order control device,
A request step which transmits said successful-bidder information to a certificate authority, and requires transmission of a public key corresponding to said secret key,
Verification steps which verify the justification of said signature information using said public key transmitted from said certificate authority according to a demand by processing of said request step,
A storage control step which makes an information management chip delivered with said goods memorize delivery pertinent information about delivery of said goods when the justification of said signature information is checked by processing of said verification steps
****** -- a delivery management method characterized by things.
[Amendment 3]

[Document to be Amended]Description
[Item(s) to be Amended]0001
[Method of Amendment]Change
[The contents of amendment]
[0001]
[Field of the Invention]
contents [of the load in which especially this invention has been delivered about a verification system and a method, an information processor and a method, an order control device and a method, a distribution control device, and a method], and delivery origin -- or, It is related with the verification system and the method, the information processor and the method, the order control device and the method, distribution control device, and method of enabling it to check easily and certainly the justification of various information about delivery of loads, such as a delivery trader.
[Amendment 4]
[Document to be Amended]Description
[Item(s) to be Amended]0016
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 5]
[Document to be Amended]Description
[Item(s) to be Amended]0019
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 6]
[Document to be Amended]Description
[Item(s) to be Amended]0021
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 7]
[Document to be Amended]Description
[Item(s) to be Amended]0022
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 8]
[Document to be Amended]Description
[Item(s) to be Amended]0024

[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 9]
[Document to be Amended]Description
[Item(s) to be Amended]0026
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 10]
[Document to be Amended]Description
[Item(s) to be Amended]0027
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 11]
[Document to be Amended]Description
[Item(s) to be Amended]0029
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 12]
[Document to be Amended]Description
[Item(s) to be Amended]0030
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 13]
[Document to be Amended]Description
[Item(s) to be Amended]0031
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 14]
[Document to be Amended]Description
[Item(s) to be Amended]0033
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 15]
[Document to be Amended]Description
[Item(s) to be Amended]0034
[Method of Amendment]Deletion

[The contents of amendment]
[Amendment 16]
[Document to be Amended]Description
[Item(s) to be Amended]0035
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 17]
[Document to be Amended]Description
[Item(s) to be Amended]0036
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 18]
[Document to be Amended]Description
[Item(s) to be Amended]0037
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 19]
[Document to be Amended]Description
[Item(s) to be Amended]0038
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 20]
[Document to be Amended]Description
[Item(s) to be Amended]0039
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 21]
[Document to be Amended]Description
[Item(s) to be Amended]0040
[Method of Amendment]Deletion
[The contents of amendment]
[Amendment 22]
[Document to be Amended]Description
[Item(s) to be Amended]0043
[Method of Amendment]Change
[The contents of amendment]

[0043]
In the information processor and method of this invention, the public key corresponding to the secret key saved by the information management chip delivered with goods is acquired, and random information is generated. The generated random information is transmitted to an information management chip via short-distance-radio communication, it is received via short-distance-radio communication, and the signature information generated as a thing corresponding to random information by an information management chip is verified using a public key.
[Amendment 23]
[Document to be Amended]Description
[Item(s) to be Amended]0044
[Method of Amendment]Change
[The contents of amendment]
[0044]
In the order control device and method of this invention, The merchandise information containing the identification information of goods, and User Information about the order Lord of goods, And ordering information including the 1st signature information corresponding to merchandise information and User Information generated using the 1st secret key saved by the information processor is received, User Information is transmitted to a certificate authority, and transmission of the public key corresponding to the 1st secret key is required. An information processor is notified that the order was materialized, when the justification of the 1st signature information is verified and the justification of the 1st signature information is checked using the public key transmitted from the certificate authority according to a demand.
[Amendment 24]
[Document to be Amended]Description
[Item(s) to be Amended]0045
[Method of Amendment]Change
[The contents of amendment]
[0045]
In the distribution control device and method of this invention, The merchandise information containing the identification information of goods, User Information about the order Lord of goods, . Were generated using the secret key saved by the successful-bidder information about the administrator of an order control device, and an order control device. Delivery request information including merchandise information, User Information, and the signature information corresponding to

successful-bidder information is received, and transmission of the public key corresponding to a secret key in transmission is required of a certificate authority in successful-bidder information. When the justification of signature information is verified and the justification of signature information is checked using the public key transmitted from the certificate authority according to a demand, the delivery pertinent information about delivery of goods is memorized by the information management chip delivered with goods.

[Amendment 25]

[Document to be Amended]Description

[Item(s) to be Amended]0046

[Method of Amendment]Deletion

[The contents of amendment]

[Translation done.]